Calhoun: The NPS Institutional Archive

DSpace Repository

Theses and Dissertations 1. Thesis and Dissertation Collection, all items

1982

A distributed network supporting ocean surveillance.

Vassiliou, Stavros.

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/20132

Downloaded from NPS Archive: Calhoun

Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

http://www.nps.edu/library

DUDLEY KNOX LIBRARY
NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIF. 93940

NAVAL POSTGRADUATE SCHOOL

Monterey, California

THESIS

A DISTRIBUTED NETWORK
SUPPORTING OCEAN SURVEILLANCE

by

Stavros Vassiliou

October 1982

Thesis Advisor: U. R. Kodres

Approved for public release, distribution unlimited

T206922

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS
BEFORE COMPLETING FORM

1. REPORT NUMBER
2. GOVT ACCESSION NO.
3. RECIPIENT'S CATALOG NUMBER

4. TITLE (and Subtitle)
A Distributed Network Supporting
Ocean Surveillance

5. TYPE OF REPORT & PERIOD COVERED
Master's Thesis;
October 1982

6. PERFORMING ORG. REPORT NUMBER

7. AUTHOR(s)
Stavros Vassiliou

8. CONTRACT OR GRANT NUMBER(s)

9. PERFORMING ORGANIZATION NAME AND ADDRESS
Naval Postgraduate School
Monterey, California 93940

10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS

11. CONTROLLING OFFICE NAME AND ADDRESS
Naval Postgraduate School
Monterey, California 93940

12. REPORT DATE
October 1982

13. NUMBER OF PAGES
170

14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)
Naval Postgraduate School
Monterey, California 93940

15. SECURITY CLASS. (of this report)
Unclassified

15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release, distribution unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Multicomputing, Fiber-optic, Data partitioning, Command, Control and Communications (C3), Real-time, Distributed network, Ring architecture

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

This thesis demonstrates the improvements in computational efficiency, expandability, flexibility and cost that can be achieved in the solution of the Ocean Surveillance problem by the use of recently introduced technology. A preliminary design of the surveillance portion of a conceptual model of a fault tolerant distributed Command, Control and Communications system

DD FORM 1473 1 JAN 73 EDITION OF 1 NOV 65 IS OBSOLETE
S/N 0102-014-6601

Block #20 Contd.

is carried out. The proposed system consists of a long haul fiber-optic ring network. Each one of its nodes has a similar multicomputer architecture for the manipulation of data collected by a variety of detection sensors. The performance prediction of the proposed model is included as well.

Approved for public release, distribution unlimited

A Distributed Network
Supporting Ocean Surveillance

by

Stavros Vassiliou
Commander, Hellenic Navy
B.S., Hellenic Naval Academy, 1965

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
October 1982

73423
e

NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIF. 93940

ABSTRACT

This thesis demonstrates the improvements in computational efficiency, expandability, flexibility and cost that can be achieved in the solution of the Ocean Surveillance problem by the use of recently introduced technology. A preliminary design of the surveillance portion of a conceptual model of a fault tolerant distributed Command, Control and Communications system is carried out. The proposed system consists of a long haul fiber-optic ring network. Each one of its nodes has a similar multicomputer architecture for the manipulation of data collected by a variety of detection sensors. The performance prediction of the proposed model is included as well.

TABLE OF CONTENTS

I. INTRODUCTION ---------------------------------- 13

A. GENERAL ---------------------------------- 13

B. PURPOSE OF THESIS ---------------------------------- 16

C. C3 SYSTEMS ---------------------------------- 17

D. DISTRIBUTED MICROCOMPUTER SYSTEMS (REVIEW) ---- 24

E. PROPOSED C3 SYSTEM'S CONCEPTUAL MODEL --------- 29

F. THESIS ORGANIZATION ---------------------------------- 31

II. SYSTEM'S ARCHITECTURE ---------------------------------- 34

A. OVERVIEW ---------------------------------- 34

1. Network Organization -------------------- 36

2. Sensors/Weapons Systems ------------------ 38

3. Multicomputer Nodes ---------------------- 38

4. Fiber-Optic Ring Interface Network -------- 40

B. SENSORS ---------------------------------- 42

1. Subarea Physical Sensor Coverage ---------- 44

2. Sensor Interconnection to the Network ----- 46

C. MULTICOMPUTER NODES ---------------------------------- 49

1. Single Board Computers (SBC) -------------- 51

2. System's Bus ---------------------------------- 51

D. FIBER-OPTIC RING INTERFACE ------------------- 54

1. Description ---------------------------------- 54

2. Fault Tolerance ---------------------------------- 58

III. DATA STORAGE AND DATA FLOW BETWEEN NODES IN THE NETWORK OF THE C3 SYSTEM ---------------- 62

A. GENERAL -- 62

B. STATIC DATA ------------------------------------ 64

1. Data Categories --------------------------- 64

2. Data Relationships ------------------------ 68

3. Storage Requirements ---------------------- 68

4. Response Times ---------------------------- 73

C. DYNAMIC DATA ----------------------------------- 73

1. Reference Data ---------------------------- 74

2. Tracks/Reports ---------------------------- 75

3. Storage Requirements ---------------------- 77

4. Response Times ---------------------------- 80

D. DATA FLOW -------------------------------------- 81

1. Data Flow on the Network ------------------ 81

2. Data Flow Inside the Multiprocessor Node ------------------------------------ 87

E. DATA FLOW IN CASE OF FAILURES ------------------ 89

1. Link Failure ------------------------------ 90

2. Node Failure ------------------------------ 91

3. Node Interface Failure -------------------- 93

4. Network Saturation ------------------------ 94

5. Multiprocessor Node Saturation ------------ 95

IV. DATA AND PROGRAM ORGANIZATION WITHIN THE COMPUTING NODE --------------------------------- 96

A. PROCESS/TASK ORGANIZATION --------------------- 96

1. Assumptions ------------------------------- 97

2. Process Organization ------------------- 98
3. Radar Interface Module (RIM) ------------ 98
4. Local Correlation Module (LCM) ---------- 99
5. Common Region Correlation Module (CRCM) - 105
6. Scheduler Module (SM) ------------------- 109
7. Shared Memory --------------------------- 110
8. Module Integration ---------------------- 111

B. DATA CORRELATION -------------------------- 113
1. Clarifications -------------------------- 115
2. Overall Correlation --------------------- 116
3. Report-to-Report Correlation ------------ 120
4. Report-to-Track Correlation ------------- 123
5. Track-to-Track Correlation -------------- 124

C. TRACK IDENTIFICATION ---------------------- 125
1. Track Record Format --------------------- 125
2. Track Number Allocation ----------------- 126

D. TACTICAL SITUATION ASSESSMENT ------------- 127

E. THE HUMAN INTERFACE ----------------------- 130
1. Hardware -------------------------------- 132
2. Process Organization -------------------- 133

F. COMPONENT FAILURE DIAGNOSIS AND SYSTEM REORGANIZATION ----------------------------- 133
1. Node Bus Failure ------------------------ 134
2. Sensor Failure -------------------------- 134
3. SBC Failures ---------------------------- 135
4. Shared/Common Memory Failure ------------ 136

G. OVERLOADS AND SYSTEM'S RESPONSE ------------ 136

V. PERFORMANCE PREDICTION AND EVALUATION ---------- 140

A. LINEAR PERFORMANCE IMPROVEMENTS WITHIN THE NODE ------------------------------- 140

B. PERFORMANCE IMPROVEMENTS BY ADDING A NODE TO THE NETWORK ------------------------ 145

C. COMPARISONS WITH EXISTING SYSTEMS ---------- 146

1. Failure Tolerance ---------------------- 146

2. System Expansion ----------------------- 147

3. Programming Ease ----------------------- 148

VI. CONCLUSIONS ---------------------------------- 149

A. EXTENDABILITY OF PROCESSING POWER ---------- 149

1. Multicomputing ------------------------- 149

2. Area Partitioning ---------------------- 150

B. FAILURE TOLERANCE -------------------------- 151

1. Fault Tolerance at the Node Level ------ 151

2. Fault Tolerance at the Network Level ---- 152

C. MISCELLANEOUS ------------------------------ 153

D. RECOMMENDATIONS ---------------------------- 154

APPENDIX A: CONCEPTUAL DATA STRUCTURES AND RELATIONS - 156

1. Data Structures ---------------------------- 156

2. Data Relations ----------------------------- 162

LIST OF REFERENCES ---------------------------------- 165

INITIAL DISTRIBUTION LIST --------------------------- 169

LIST OF TABLES

II-1. Metallic Cable Links Versus Fiber-Optic Links -- 57

III-1. Match and Accept Bits ------------------------- 82

LIST OF FIGURES

I-1. Chronological Sequence of Event Handling in C3 ---------- 15

I-2. Examples of Connection Topologies for Multipath Networks ---------- 26

I-3. Inter-Node Network and Subarea Network ---------- 30

II-1. System's Topology ---------- 35

II-2. Network Layout ---------- 37

II-3. Connection of Sensors/Weapons to the Network ---------- 39

II-4. Internal Multiprocessor Node Architecture ---------- 40

II-5. Rona's Canonical Model ---------- 43

II-6. Subarea Radar Network Coverage ---------- 45

II-7. Sensor Connection to Network ---------- 48

II-8. Multiprocessor Module Group Arrangement ---------- 50

II-9. Radar Module Complex ---------- 52

II-10. Loop Interface Operation ---------- 59

II-11. Standby Channel Mechanism ---------- 60

III-1. GDB Custodian Facility Operation ---------- 71

III-2. New Report Data in GDB ---------- 72

III-3. Track Record Structure ---------- 76

III-4. Relation of TRACK to PLOT ---------- 77

III-5. New Data in the GDB ---------- 84

III-6. Request Satisfaction by the GDB ---------- 84

III-7. Collaborating Nodes ---------- 85

III-8. Global Data Base Update with Dynamic Data ----- 86

III-9. Data Flow Inside the Multiprocessor Node ------ 89

IV-1. Time Sequence of Processes in the Radar Module Complex ---------------------------------- 96

IV-2. Radar Interface Module ------------------------ 99

IV-3. Local Correlation Module --------------------- 102

IV-4. Local Correlation Module Internal View -------- 103

IV-5. Common Region Correlation Module ------------- 106

IV-6. Internal View of Dual CRCM ------------------- 107

IV-7. Internal View of Triple CRCM ----------------- 108

IV-8. Shared Memory Division ----------------------- 111

IV-9. Integrated System's View --------------------- 112

IV-10. Time Analysis of Events ---------------------- 113

IV-11. Morefield's Method --------------------------- 117

IV-12. Initial Picture ------------------------------ 119

IV-13. Well-Behaving Tracks ------------------------- 119

IV-14. Second (final) Pass -------------------------- 119

IV-15. Heading Unknown ------------------------------ 121

IV-16. Heading Known -------------------------------- 122

IV-17. Flowchart for Multi-target Multisensor Correlation ---------------------------------- 129

IV-18. Human Interface Module Complex --------------- 131

IV-19. Relaxing Process Mechanism ------------------- 138

V-1. Time-Line Analysis with One SBC -------------- 141

V-2. Time-Line Analysis with Four SBCs ------------ 142

V-3. Time-Line Analysis with Eight SBCs ----------- 143

VI-1. Conceptual Levels of Bussing ----------------- 150

ACKNOWLEDGEMENT

I would like to express my sincere appreciation to my thesis advisor, Uno Kodres, for his inspiration and expert guidance during this undertaking. The friendly atmosphere that was created among us helped me a lot during my work.

Also, I would like to thank my wife, Eva, for the long waiting nights she spent during my thesis quarters.

I. INTRODUCTION

A. GENERAL

Any Command, Control and Communications (C3) system must be able to successfully perform the following basic functions:

1. Detection of targets within its surveillance area limits by means of various search sensors. These sensors may be mounted on mobile or fixed platforms.

2. Tracking of targets, as long as they remain within the geographical area of interest. This is achieved by the use of fixed or mobile tracking systems.

3. Classification of targets after detection by means of identification devices and/or association of present to previously obtained information.

4. Display positional information considering all targets within the surveillance area limits onto plots and/or large screen displays.

5. Storing tactical information into data bases for use in the near or more distant future.

6. Control of weapon and support systems, to attack the target(s) after permission has been granted. This is accomplished by providing target behaviour parameters to the Fire Control Systems (FCS) and the various defensive systems such as Electronic Support Measures (ESM), Electronic Countermeasures (ECM), decoys, etc.

The difficulty of accomplishing the above functions varies significantly depending on:

a. The technological advance in each of the referred application areas.

b. The effectiveness of human interaction with the system (training, motivation and emotional factors).

Today's trend is to replace the functions formerly performed by humans with computer controlled functions, up to the point of leaving to the humans only the ultimate decision making function, and the option to override the system (authorized personnel).

All functions of the C3 systems have undergone development over the last twenty years and many computer applications have been successful. For instance, a computer can automatically "read" information directly from the radar receiver, make the conversion of its coordinates (polar to Cartesian), plot, track, store the information into a database and, if desired, feed data to a weapons control system to enable it to destroy the target.

A surveillance system acts as part of a C3 system which handles the functions of detection, tracking, classification and information storing [Ref. 1]. Detection of an object should always result in alerting the decision maker. This can be done through means of information display. Figure I-1 illustrates how a surveillance system fits in the process of handling a typical "event" [Ref. 2].

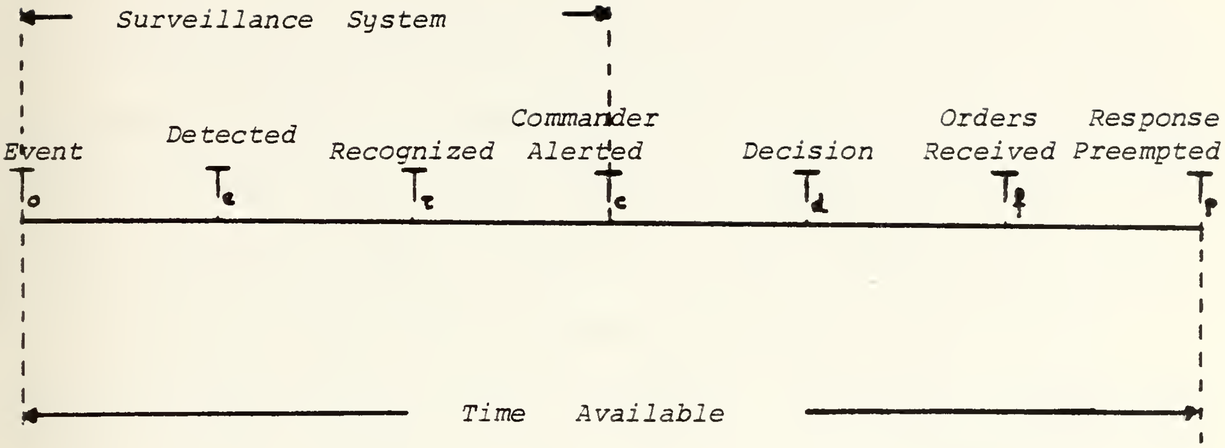


Figure I-1. Chronological Sequence of Event Handling in C3.

After the Commander has been alerted, a decision on the appropriate reaction to the threat is made. This function can be accomplished either as a pure human aided decision or as an automated response process (Aegis system).

Communications will ensure that the above decision is transmitted and received in such a way that delays are minimized and message context is highly reliable. This way the orders will be received "in time" and the decided response will be initiated.

Finally, the Commander should be equipped with mechanisms and procedures enabling him to control the correct execution of the issued orders. These procedures reflect the second element of the C3 triad, namely the "control".

B. PURPOSE OF THESIS

The purpose of this thesis is to explore the use of the recently developed Large Scale Integrated (LSI) circuit technology, the fiber-optic communications technology and some newly developed operating systems concepts in order to build a Command, Control and Communications (C3) system. The thesis offers a preliminary design of the surveillance portion of such a C3 system which is based on a distributed local network concepts and which contains processing nodes of the network built from multi-microcomputer systems. The network nodes are tied together with a fiber-optic double ring structure which permits single failures of either a link or a computational node without causing system's failure. The network nodes consist of a multiprocessor system of single board computers (SBC) sharing common memory for shared data. The operating system of each network node is distributed among the SBC's in the node and the operating system of the network is an extension of the operating system at each network node.

The advantages such a system offers are:

1. Failure tolerance at both the network and node levels.
2. Computation load balancing.
3. Expandability at both the network and node levels.
4. Low hardware cost.
5. High system capacity.
6. Increased survivability (through decentralization).

On the other hand, the price that has to be paid is expressed in the following drawbacks:

7. The proposed architecture is untried (high risk).
8. The operating system becomes more complex as a result of the implementation of data and process distribution (in contrast to the ones used in centralized systems).

To demonstrate how the above concepts can be implemented, a simplified model of a Tactical Surveillance System will be described. The design of the system will be applicable to most geographical environments and will be based on some ideas expressed in the open literature on surveillance systems plus the author's 21 years of experience in Naval Tactics.

C. C3 SYSTEMS

Some of the existing Command, Control and Communications (C3) systems will be overviewed in this section. Most of these systems are operational today. Since they belong to different generations, they will be described in a chronological order. They, in some respect, reflect the state-of-the-art in both hardware and software during the time period they were designed.

As an aggregate Naval system, C3 touches on a number of related functions such as intelligence, surveillance, navigation and logistics. A C3 system must provide the means whereby military decision makers have access to the information that these other functions provide. So, most of the C3 systems which are in operation today are tightly or loosely

linked with systems dedicated to one or more of these related functions.

Going back to the mid 50's, the three services of the U.S. Armed Forces were greatly concerned with the threat from high speed aerial attacks. They contracted with the University of Illinois Control System Laboratory to explore the use of digital computers for the rapid solution of the air defense problem using information received and correlated from a network of search radars [Ref. 3]. The growing threat to forces afloat and ashore, coupled with the diminishing time available to react, spurred the investigation of computer assistance for C3 from World War II on. Up to then, various attempts to adapt the technology of analog computers had unsatisfactory results. The systems were complex, limited in capacity and had little potential for growth. The new era gave rise to some successful C3 systems.

1. Semi-Automatic Ground Environment (SAGE) System

It was designed by IBM for the Air Force and is still operational. It consists of a network of air search radars all over northern U.S. and Canada.

The central computer of the system has data on positions of both friendly and enemy aircraft (weapons, interceptors, readiness, fuel, etc.) so as to keep a continuous track on them and enable the coordination of the air defense activities.

2. Naval Tactical Data System (NTDS)

It was developed in the late 50's to early 60's period. It operates in the Task Force environment but each ship has a suite of equipment that can function as a self-sufficient system. One of the biggest obstacles of the system in building networks for the exchange of target information is the limited memory capacity of the computers used. The system's major components are:

a. Analog to Digital (A/D) Converters

They convert analog sensor data into digital information in order to be entered into the computer.

b. Computing Equipment

A multicomputer installation is used because of the limitations on core size and the need to store everything in memory (programs, data, and messages). Univac computers are used.

c. Communications Equipment

All elements of a Task Force or several Task Forces are able to exchange information rapidly over high-speed data links (high level of data integration).

d. Visual Displays

There exist display consoles for detecting, tracking, identifying, evaluating and assigning weapons for intercept control.

Both hardware and software (build in modules) have gone through a series of improvements which shortened

response times by sharply reducing the human role in data processing and presentation.

3. Airborne Tactical Data System (ATDS)

The development of transistorized computers small enough to fit in airplanes, permitted the development of the ATDS. Its purpose is to provide an independent, self contained detection, identification, tracking and air controlled intercept capability for the picket aircraft. The system interfaces with the NTDS. Its sensor is a search radar.

The data processing and display functions are performed by a computer which embeds two processors that share the program functions, and three cathode ray tube display units for the crew. The computer processes track data, either for transmission to the NTDS or to be used for the control of interceptors. All computer programs are modularly built and divided into several classes and subclasses which are handled by one or both processors of the computer.

In both NTDS and ATDS, as in all equivalent C3 systems of this generation, the greatest concerns have been: hardware reliability, memory size limitations, system interfacing and maintainability [Ref. 4]. The centralized processing concept was popular, since only a major computer installation made the operational and maintenance functions economically and technically feasible (specialized personnel, spare parts, etc.).

The computers used in these systems reflect the architecture and technology of the 60's and are difficult to be integrated into a larger system. On the other hand, the substitution of analog with digital computers has increased the performance of these C3 systems.

To form the database for these systems, data from many other systems are utilized. These other systems are designed for their own specific purposes and a lot of changes had to be made for data to be interchangeable.

From the software point of view, data are manipulated sequentially since it was assumed that the method of their arrival is sequential too [Ref. 5].

In general, it can be stated that SAGE, NTDS and ATDS systems are basically manual systems, strongly assisted by computers [Ref. 6].

4. Ocean Surveillance Information (OSIS) System

It is a world-wide network of facilities and analysts that provides comprehensive information on everything of interest which lies on, over and under the sea. It uses a digital network to gather, correlate and disseminate information, primarily for strategic headquarters commanders. The system was designed in the late 60's. Contact data classification and identification is sped up by the use of heuristic criteria that assign confidence weights to them.

5. Outlaw Shark

Similar to the OSIS system, it is still under test on a number of Navy vehicles and selected shore stations.

6. Octopus Tracking System

It is an experimental passive sonar tracking system.

7. Intelligence Tracking and Correlation (ITAC) System

The system operates within a surveillance data base which maintains separate track files for each sensor that provides data. The system is still in the testing phase.

The above constitute a later generation of C3 systems. Their detailed architecture is unknown to the author because of their classification level. What is known is that they all use large or mini computers as processing devices and distributed processing is probably not used in any one of them. As for the software, all information is covered under the classifications "SECRET" or "CONFIDENTIAL".

8. Aegis Combat System (ACS)

It is a sophisticated antimissile and antiair C3 system which is being installed onboard several ships of the U.S. Navy. The system in its present version contains 15 AN/UYK-7 and 24 AN/UYK-20 mini computers. These computers can operate as cooperating independent units or in groups of up to 4 AN/UYK-7 processors in a multiprocessor system. Each computer system is dedicated to a major function such as processing sensor information, controlling the radar, or coordinating the weapons systems. The total hardware cost

of these computers is about $5,000,000. Timely control of an Aegis ship's missile fire-power during a multi-axis surprise attack does not always leave room for positive human control [Ref. 7]. Therefore, Aegis has a pre-selected operating mode in which the system itself makes the tactical decision to engage, based on given threat criteria.

9. Navy Command and Control System (NCCS)

It is a loose confederation of relatively autonomous command and control nodes. Its development was started in the mid-70s and it is scheduled to perform as a response but flexible system subordinating the goals of individual components to those of a larger organization (nationwide). It attempts to take full advantage of sophisticated systems that already exist within the U.S. Navy command structure. The nodes of the system correspond to command posts ashore and afloat. The new nodes differ from those they are replacing primarily in terms of their processing capacity and the speed and clarity of their data presentations. The system is still under development.

It is apparent that the U.S. Navy is still using computers that reflect the architecture and the technology of the 60's which are difficult to use as components in larger systems. The inter-connections between the subsystems are achieved by ad hoc cabling between these computers which must share information. On the other hand, automated naval C3 is becoming a reality despite problems of reliability

and efficiency that still appear from time to time. Automation has become more and more routine for military tasks, and reliability has improved as operators and users accustom themselves to the new systems.

As expressed in Chapter 9 of [Ref. 7], future C3 systems will take advantage of Large Scale Integration (LSI), multicomputer systems (instead of central large computers) and processing distribution architectures. Future systems will also be potentially less expensive in hardware costs than the existing ones.

D. DISTRIBUTED MICROCOMPUTER SYSTEMS (REVIEW)

In general, military Command, Control and Communications systems of today fall in the category of large-scale distributed, event driven systems (from the operational point of view). The problem of C3 system design is one of optimizing, on a system's wide basis, the aggregation of data coming from geographically distributed sensors and decision makers subject to limits on communications and computation [Ref. 42]. Since the various decision makers (users) have disparate information needs and practical considerations make it impossible to supply the global information set to each user, the desirable architecture is one that includes sensor, processor and communications resources that provide each user just the information needed at just the right time.

There does not yet exist a unique definition for a distributed system. However, viewing the centralized system

(all functions are controlled by a central computer) on one hand, and the decentralized system on the other (functions are performed by individual processors with no coordination), distributed systems can be placed somewhere in between. In other words, they can be defined as decentralized systems where process coordination can be applied. Their main characteristics are:

1. Modular and extensible architecture.
2. Arbitrary number of system and user processes.
3. Communication is by message passing or shared memory.
4. There exists a system control supporting interprocess cooperation and runtime management.
5. Interprocess messages have non-zero, variable and sometimes unpredictable delays.

Applications where the implementation of distributed systems is recommended are these in which there already exists a geographical dispersion. In this case the distributed systems allow for fast exchange of data among the nodes, balancing of processing load, increased system survivability and great flexibility in computation.

A carefully designed distributed system reflects an almost failure proof processing/data-storing potential, combining most of the advantages of centralized and decentralized systems.

The greatest concern in distributed systems involves communications. Modern hardware/software state-of-the-art has made it possible to overcome most of the previously

existing communications obstacles. Much research is done today towards the improvement of the performance of distributed systems; however, many problems, including the problem of centralized or decentralized controls, remain unresolved.

There are various kinds of networking architectures which can be used in distributed systems. Figure I-2 shows the most common ones.

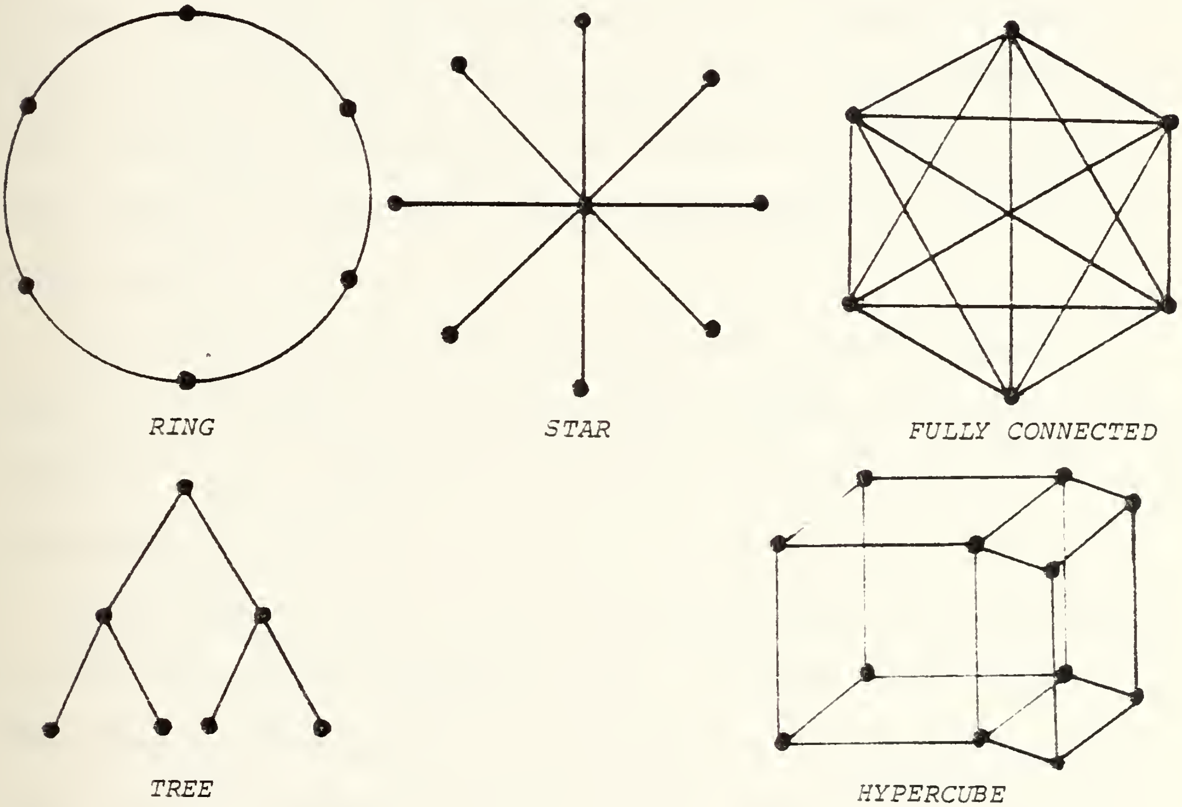


Figure I-2. Examples of Connection Topologies for Multipath Networks.

No working distributed C3 system is currently in operation. However, there exist some banking, airline reservation and computer network systems (ARPANET, DECNET, etc.) which are distributed. Some more are currently going through their experimental phase and others are under development. The above facts necessitate a more or less theoretical or a heuristic approach to the problem of finding the most appropriate network architecture for a C3 system.

In general, distributed network architectures can be divided into local and long-haul ones. Because of the recent advances in fiber-optic technology, it is likely that some local network architectures can be used in systems where the nodes are dispersed in wide areas (several thousands of square iles).

The factors which are considered in choosing one of the above architectures are performance, communications and data transfer costs, communications delay, expandibility and file availability.

Performance can be further analyzed into data throughput on the network and response time. It maybe is the most important consideration in the design of real-time systems. From the above network architectures, the one that offers the higher throughput and fastest responsiveness, is the fully connected one since each one of the nodes is directly connected to all the others. Second to the fully connected, the ring and hypercube architectures have good performance characteristics. The rest of the architectures are inferior.

Considering the communications cost for the "star", "ring", "completely connected", "tree", and the "hypercube" networks, it appears that the ring network is more economical in terms of communications lines and interface units cost [Refs. 44, 45].

In terms of data storage cost the differences between all of the networks shown in Figure I-2 are not significant. The star topology seems to be more convenient and economical if a simple duplication of data storage is chosen.

Communications delay varies a lot between these architectures. A fully connected network minimizes delays. The use of fiber optics can reduce communications delays since the velocity of data transmission is practically equal to the speed of light. The other aspect of communications delay is how long should some data have to wait in a queue to succeed in accessing a (shared) communications means (e.g. a bus).

The ring network is much superior to all the others in terms of expandibility since very few changes are required to be made (in software and in the hardware) whenever a new mode is added to the network.

The file availability in the star network architecture is the worst because of the long queues that can be formed in the ports of a central global database (which is normally hosted at the central node of the network).

E. PROPOSED C3 SYSTEM'S CONCEPTUAL MODEL

The Command, Control and Communications (C3) system which is described in this thesis has the following general characteristics:

1. There exists a geographical ocean area of approximately 400,000 square Km, which has a number of islands and islets spread within its limits and is constantly under surveillance by a number of fixed radars.

2. Command and Control activities are distributed among four Subarea Commands, each one of which controls an almost equal size subarea.

3. All subarea control centers are tied together on a distributed fiber-optic ring network permitting the full or partial integration of the tactical information handled in the local subarea environments.

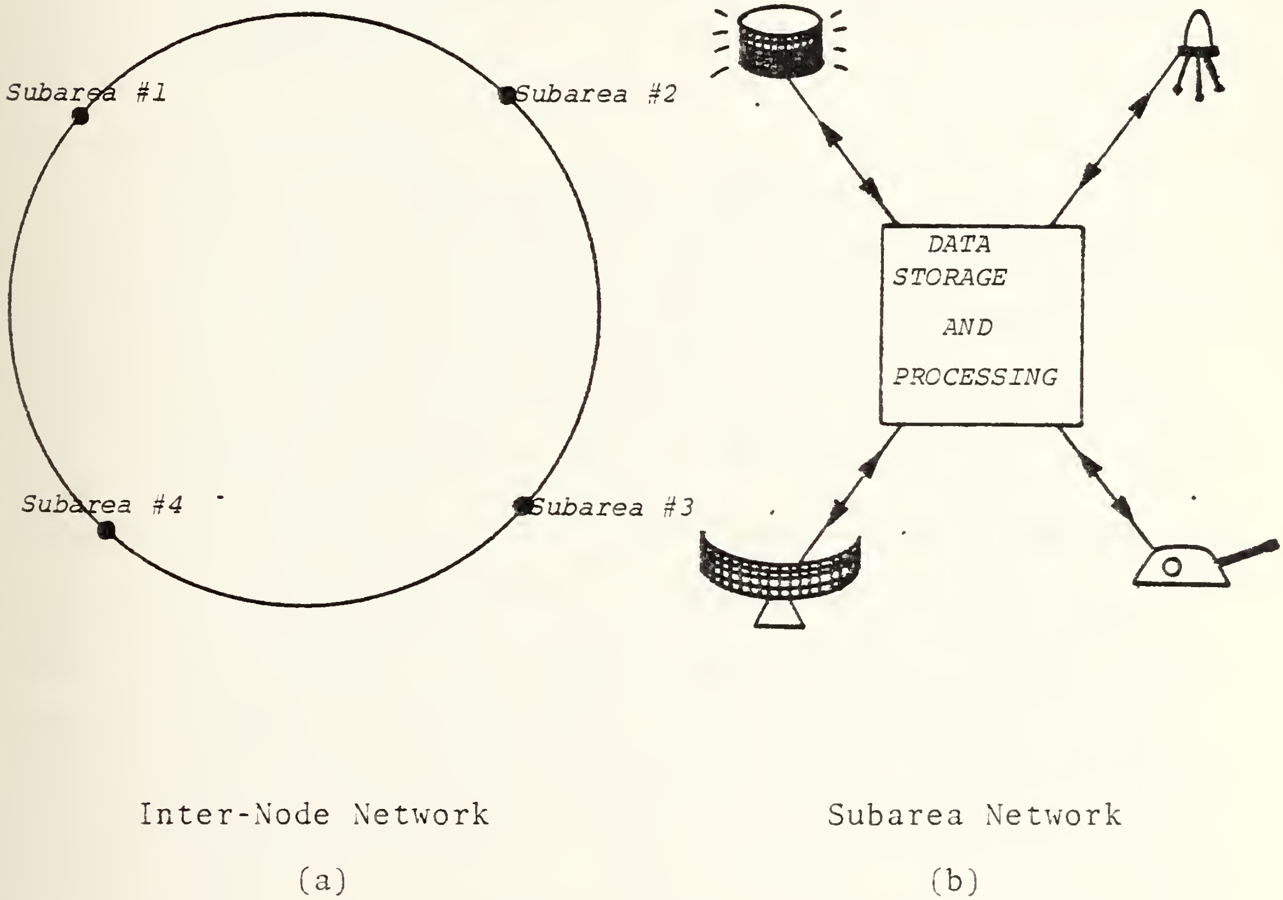
4. In every subarea there exists a local radar surveillance network. Data sensed by these radars are transmitted to a common physical site, where a complex of processors is used for the correlation of target data.

5. An identical hierarchy of software modules exists in every subarea processing site. These modules serve a standard process package and update a local database holding data that have to do with the subarea tactical environment only.

6. A global database (two or more copies) exists in one or more area sites. This database includes data concerning

all individual subareas as well as historical and "library" data.

7. Through special message passing it is possible that C3 coordination for two or more nodes be exercised by one of them. This becomes necessary whenever the geographical extent of the operation in progress exceeds the limits of an individual Subarea or when a Subarea Command is unable to exercise its C3 functions (failure).



Inter-Node Network

(a)

Subarea Network

(b)

Figure I-3. Inter-Node Network and Subarea Network

8. A variety of failure tolerance mechanisms (hardware and software) have been designed into the proposed system. These are the duplication of the fiber-optic ring cable, the existence of alternate sensor/weapons systems connections to other subarea nodes, the duplication of the global database, the load sharing mechanisms between the processors of each multicomputer node, etc. All of them contribute to reducing the possibility of an occurrence of a fatal failure in the system.

Figure I-3 gives an illustration of the system's architecture in general.

F. THESIS ORGANIZATION

The thesis is composed of six chapters.

Following the introduction, Chapter II discusses the architecture of the conceptual model of the C3 system. A system's overview is given presenting the organization of the distributed internode network, the structure of the multicomputer nodes and the fiber-optic ring interface network. A more detailed description of sensor interconnection to the network (through the computational nodes) is given. The description of the architecture of the multicomputer nodes and the fiber-optic ring interface are given in the last part of this chapter.

Chapter III deals with the C3 system's conceptual data organization (for the surveillance portion only. It includes

the identification of the conceptual data and their relationships, the description of the storage model and the organization of the "global" and "local" databases as well as the mechanisms used for information sharing among them. The flow of data in the network and the mechanisms supporting fault tolerance for the cases of failed network components are separately examined.

Chapter IV is dedicated to the organization of data and processes within the individual multicomputer nodes of the network (subarea level). This organization covers both the processing and operational requirements. It describes how the report-to-report, report-to-track and track-to-track correlation problems are handled. Track identification and the existing means for the human interface with the system are presented in separate sections. Finally the fault-tolerance of the multicomputer node is discussed.

In Chapter V a performance prediction and evaluation is attempted. Possible bottlenecks in system's operation are identified and the side effects which may be caused by expanding it are pointed out. In the last section of this chapter a comparison of this conceptual model system to existing C3/surveillance ones is done.

The final chapter is dedicated to conclusions on the extent of the research performed during the development of this thesis and recommendations for further work are expressed in relation to the goals set in Chapter I.

Appendix "A" includes illustrations of the conceptual data structures and their relationships.

II. SYSTEM'S ARCHITECTURE

A. OVERVIEW

This chapter is dedicated to the description of the architecture of the conceptual model of the Command, Control and Communications (C3) system. This model system uses as a physical background a geographical area covering ocean surface of approximately 400,000 sq. Km. The area includes a number of islands spread almost equidensely. From the command point of view, this area is partitioned into four subareas (S1 to S4). Each of these subareas has a physical, fixed command post from where the C3 functions for the subarea are exercised. A number of sensors and weapons systems (both fixed) exists within the limits of each subarea. Area topology and subarea relative arrangement is shown in Figure II-1.

Real-time performance is another background consideration for this as for most of the C3 systems. The speed and destructiveness of modern weapons systems do not permit delays, while decision-makers organize their subordinates and get in touch with the proper superiors. To affect the outcome of an operation, "real-time" command decisions must correspond to the rapidly developing conflict situation. The command and control "nodes" (subarea command posts) that support key decision-makers must maintain efficient and, when necessary,

secure communications with other nodes in the chain of command. They must organize and access a large amount of data on the operating forces and their environment (sensors/Weapons), providing commanders with concise, real-time information on which to act.

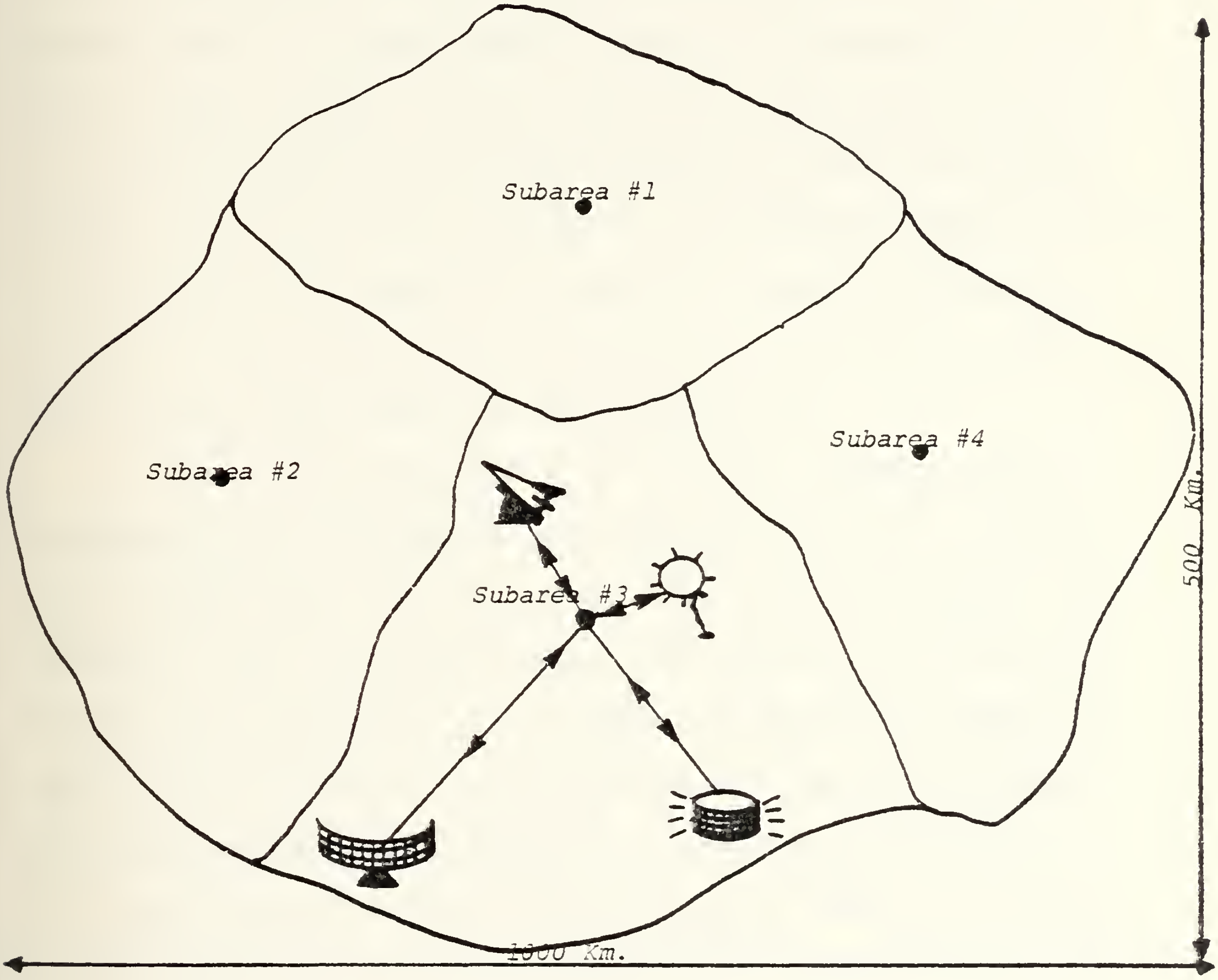


Figure II-1. System's Topology.

1. Network Organization

The four subarea command posts constitute the nodes of a fixed, double ring, distributed network. The physical channels used for internode message passing are cables of fiber-optic material which for almost all of its length is placed under water. One of the physical channels of the double ring is called "primary" and is the message traffic carrier under normal network operation. The other channel is called "standby" and is used whenever either the primary channel or a node fails. Primary and standby channels follow a different path from node to node for physical security reasons. The direction of internode message flow is unidirectional under normal network operation.

Each one of the nodes has its own, almost equal, processing power (hardware and software) so as to exercise all C3 functions. A great number (30 to 50) of Single Board Computers (SBC) of equal capabilities make up the workshop used for the execution of a family of processes accomplishing the C3 functions. Each node has its own local memory which holds all data necessary for the conduct of the C3 functions within the host subarea. Local memory is stored on hard disks and is shared among the various processes at the multicomputer node level.

In the network there also exists a so called Global Data Base (GDB) which is the internode shared memory. Two copies of the GDB exist. They are hosted in the physical

installations of every second multicomputer node. Each of the GDB copies is directly connected to the ring network and has its own computer based Data Base Management System (DBMS) [Refs. 8,9]. These DBMSs can be viewed as two extra nodes connected to the network. One of the subarea nodes acts as a "primary node" at any given time. This node is the one where the senior commander, responsible for C3 in the whole area covered by the system, happens to be (he can be in any one of the subarea command posts since they all have the same structure and potential). The internode network arrangement is shown in Figure II-2 below (see also Ref. 10: p. 24).

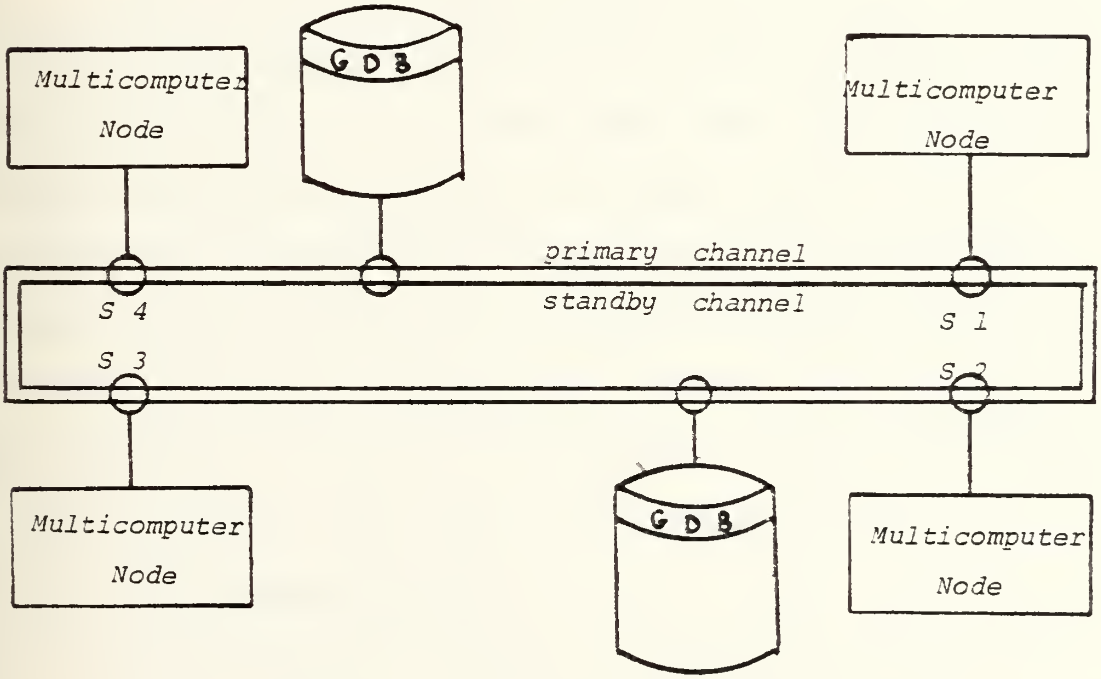


Figure II-2. Network Layout.

Message passing between the nodes occurs whenever coordination of C3 functions in two or more subareas is required, whenever the GDB is accessed or whenever messages concerning the operation of the network itself are exchanged (failures, load balancing, etc.).

2. Sensors/Weapons Systems

The C3 system has both active and passive sensors. These sensors provide the means by which "reports" are sensed and fed into the system. They are radars, electromagnetic emission detectors, underwater sonics, and optical devices.

To perform its response functions, the system controls anti-air (AA), anti-submarine (AS) as well as anti-surface (ASu) weapons and electronic/acoustical countermeasures.

Each one of the above sensors is directly connected to a node of the network which covers the C3 needs of the subarea the sensor is in. This way, four local networks of sensors and weapons systems are formed (one per subarea). In addition to these direct connections for each sensor/weapons system, there exists a secondary connection to another node (the closest). The secondary connections may be activated whenever the "parent" node fails. Figure II-3 illustrates how these connections are conceptualized.

3. Multicomputer Nodes

A multicomputer complex is physically located in every subarea command post. Thirty to fifty SBCs are interconnected through a common bus. The complex has also a

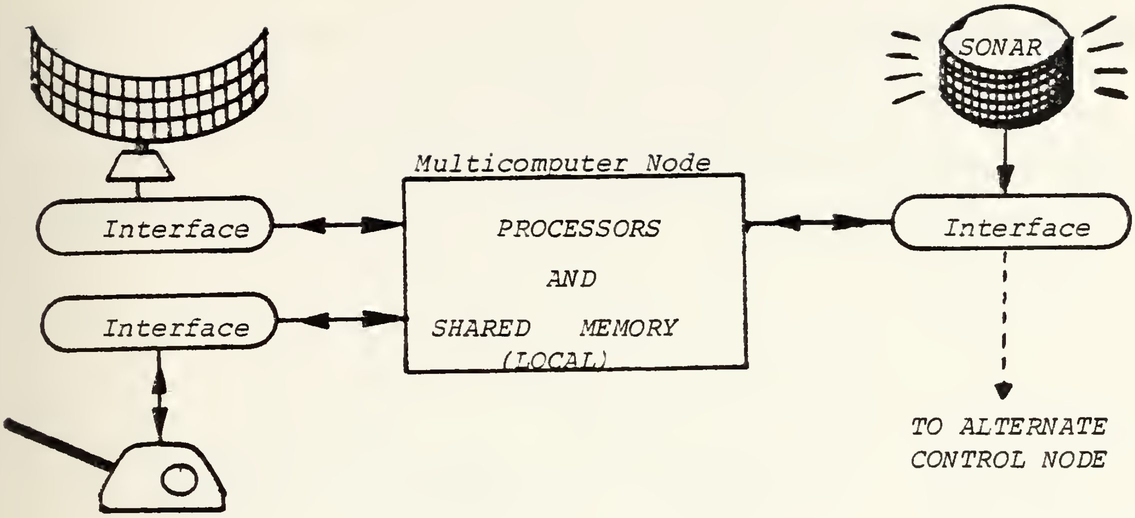


Figure II-3. Connection of Sensors/Weapons to the Network.

shared memory complex and various I/O units. The multiprocessor architecture has the characteristics of a time shared/common bus, shared memory. This architecture is based on the connection of all processing, memory and I/O units to a shared bus. Contention resolving for the use of the bus by the above units is fulfilled by a first-in first-out (FIFO) queue scheme. The most serious limitations of this organization are its reliability and the interference between units requesting the bus [Ref. 10: pp. 25-26].

To reduce contention of the various processors for the bus, private memory (RAM) and private I/O are used for the greatest possible extent. Another feature of this

application is the duplication of the bus, so a failure of this common path will not cause complete system failure. The use of the bus is limited to cross talk between processor complexes, shared memory accesses and I/O to the ring. Figure II-4 illustrates the internal architecture of the multiprocessor node.

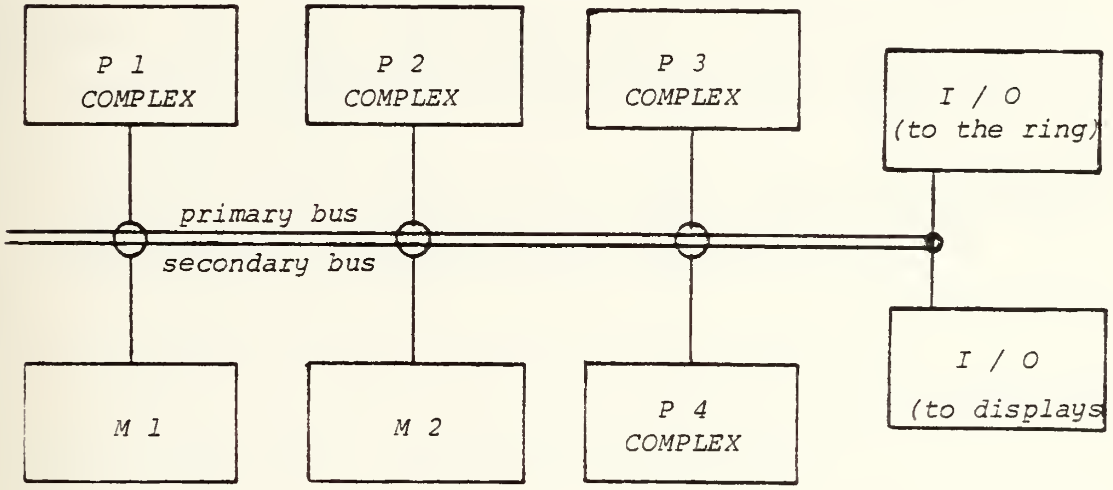


Figure II-4. Internal Multiprocessor Node Architecture.

4. Fiber-Optic Ring Interface Network

The rate of data transmission through the fiber-optic communications channel is 10Mbits/sec, which is the maximum practical rate at which the interface units of the individual nodes can operate (technology of today imposes this limit). The 1.3 μμ fiber-optic cable configuration is used. This fiber suffers less than 1db/klm signal strength loss [Ref.

16]. Repeaters are placed approximately every 20 Kms [Ref. 11] and are powered through electricity cables running parallel to the fiber-optic cable (inside the same coating). A detailed description of the technical parameters of the fiber-optic channel and the interface units used in the nodes to access it, is given in Section D of this chapter.

The advantages offered by the use of commercially available fiber-optics in communications channels over the existing coaxial and copper ones are:

a. Ability to provide extremely high data rates over long distances.

b. Lower cost of cable per kilometer (including repeater/amplifier cost). This cost is presently $0.046 per fiber meter (minimum) [Ref. 17].

c. Extremely low bit error rate (less than 10^{-9}).

d. Immunity to electrical noise, shocks and to water.

e. Low cross-talk between adjacent cables.

f. Tolerance to temperature changes (from -12° C up to 150° C). However, in underwater installations temperature varies only between 3° C and 20° C [Ref. 18].

g. Light weight, low volume.

h. High resistance to corrosion.

i. Efforts to intercept the channel are immediately detectable.

The above characteristics make the use of fiber-optic cable favorable for use in the internode ring network as communications channel because of the real-time/security/reliability requirements of the C3 system.

Fiber-optic's main disadvantages are the nonexistence of standards (affecting system's cost and parts availability), its low resistance to radiation damage, and the difficulty to make new connections of nodes on the cable (splicing the cable causes substantial strength losses). Specifically for the radiation damage, long term/low dose or high dose irradiation is causing luminescence followed by attenuation, increased dispersion and mechanical damage. These effects can be either temporary or permanent depending upon the fiber material (commercially available glass fibers are more susceptible, while germanium doped fused silica fibers appear to be the most radiation resistant [Refs. 11 and 14]. This second disadvantage of fibers is reduced by the use of underwater cable installations [Ref. 11].

B. SENSORS

The sensors of the Command and Control system are perhaps its most fundamental elements. In order that system's operation be triggered, one of the sensors has to be stimulated.

By viewing the so called Rona's Canonical general model of a Command and Control system (Figure II-5), it becomes obvious that the I/O ports through which it communicates with the environment are the sensors (stimulus set) and the weapons systems (effect set).

Since the weapons systems are less standardized, from their operational aspect, it would be unrealistic to include

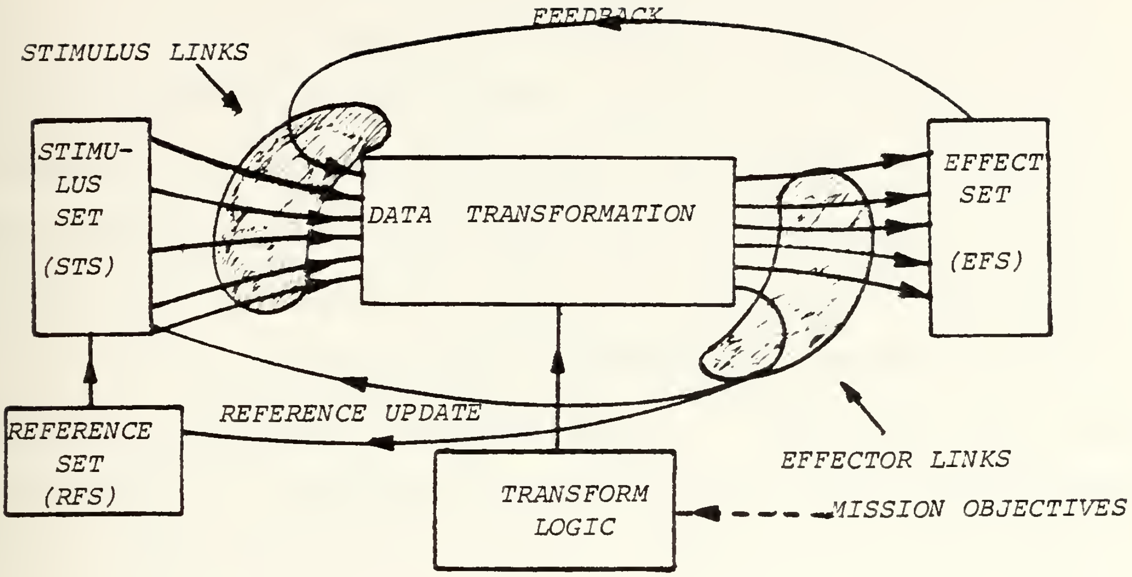


Figure II-5. Rona's Canonical Model. [Ref. 2: p. 3]

a detailed description of their interconnection to the C3 system. On the other hand, sensor's interconnection to the network will be discussed in detail.

Sensors can be considered as sources of information. However, sensors which are used exclusively for weapon control will not be considered in this section. Sensors can be categorized into the following types [Ref. 12]:

a. Continuous-valued data sensors: These are radars, sonars (both passive and active) and other tracking devices.

b. Discrete-valued data sensors: In this category, the visual detection and electromagnetic emission interception sensors can be included. Special

identification of friend or foe (IFF) equipment is also a discrete-valued data sensor.

Most of the sensors work in a periodic fashion. This period is called "scan" and it denotes the time it takes to revisit the same point in their search covered space. For instance, in the case of a radar, if it takes 6 seconds for the antenna to pass twice from a point on bearing "X", its period will be 6 seconds. The operation of the nonscanning sensors (e.g. nondirectional hydrophones) can be referred to the scan period of a scanning sensor. This way, if an event is sensed by a nonscanning sensor at time $T+\Delta T$ (in reference to the scan period of a scanning sensor), it is said that has occurred during scan period $T+1$.

The case becomes more complicated when there exist multiple scanning sensors with unequal scan periods where a lot of transformations have to be made. This added overhead slows down system's operation.

1. Subarea Physical Sensor Coverage

In each one of the subareas, the whole surface and the corresponding subsurface/air volume is covered by every one of the sensor systems applicable. For instance, a surface or air radar network should not leave any gaps (also for hydrophone, ESM, optical, etc. networks). In Figure II-6 a typical subarea conceptual radar network is shown.

Considering this radar network, the following characteristics can be observed. These also constitute the design requirements for the network.

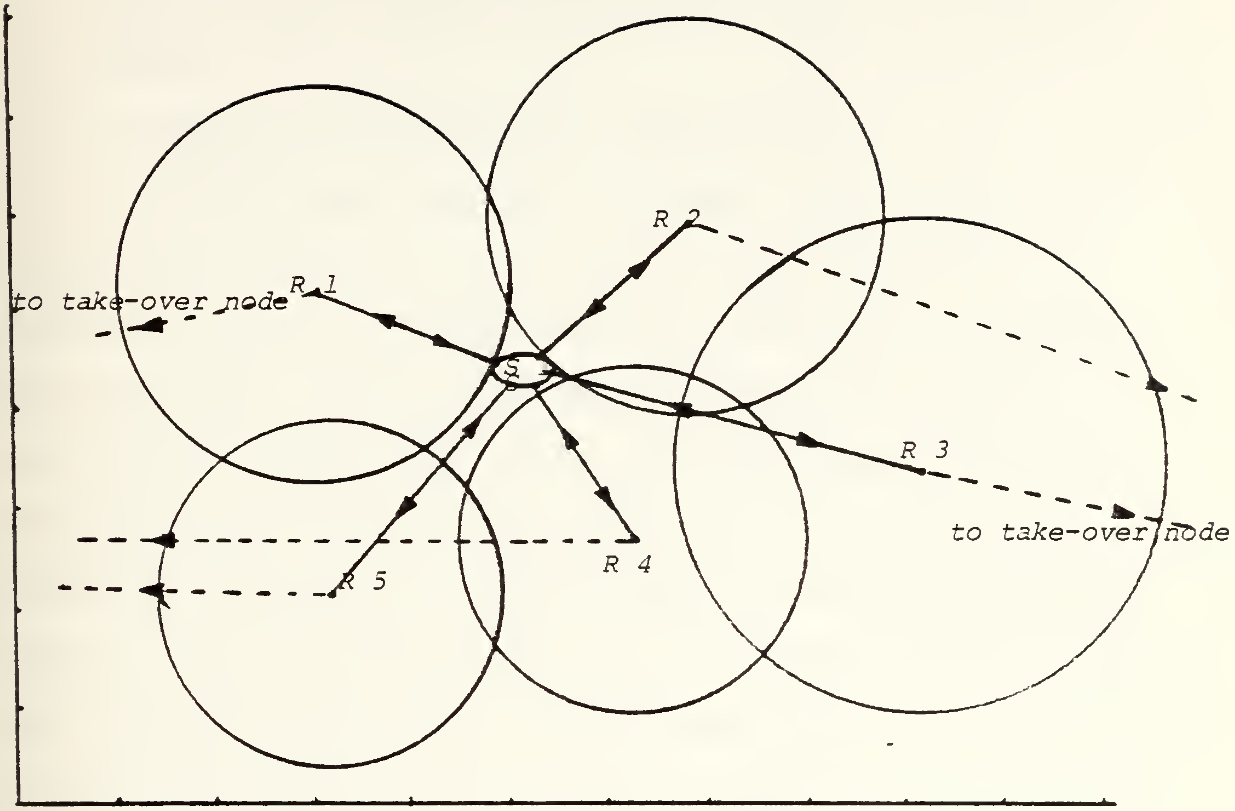


Figure II-6. Subarea Radar Network Coverage.

a. It does not leave coverage gaps.

b. It provides at least two zones of detection in terms of depth of defense (from either direction).

c. Some radar detection sectors are overlapping over the same region (at most three overlapping radar sectors).

d. Individual radar maximum detection ranges may differ.

e. A common cartesian coordinate system exists, which covers the whole C3 area. In Figure II-6 only a portion of the coordinate system is shown.

f. Another requirement, which is set in order to facilitate the report correlation process, is for all radars of a subarea to have the same scan period. Chapter IV gets into the reasoning of this decision in greater detail.

2. Sensor Interconnection to the Network

Next to each sensor (e.g. radar installation) there exists a local video monitor site. In addition, all the sensors are directly (point-to-point) connected to the multiprocessor nodes. These connections are through special interface I/O modules located at the same site. The main function of the interface modules is to convert the analog information coming from the individual sensors into digital signals. They also perform other conversions, such as they convert reports expressed in polar coordinates into cartesian (global grid) ones.

Although the cabling of the sensors to the multiprocessor nodes does not need to be of any special material, the use of fiber-optics would reduce both the data contamination and the communications delay.

Sensors are sited into fixed physical locations (land or seabed). Some of them are mobile (on vehicles) and can be moved to preselected alternate locations. These alternate locations are close to the normal ones so that when they are used the sensors/weapons coverage is not affected. The coordinates of these locations are known to the interface modules so that the conversion of the report parameters into the common cartesian grid is performed locally.

In both normal and alternate locations, cabling and power supplies already exist. The reason alternate locations have been introduced is physical security of the sensors during tension or wartime periods.

Another provision which increases the survivability of the system is the connection of all sensors, as well as weapons systems to a second multiprocessor node. This way, their control can be switched to this take-over node whenever either the node that normally controls them fails or it becomes overloaded. This reduces the possibility of gap occurrences on the surveillance coverage of the C3 system. Figure II-7 illustrates a typical sensor's connection to the network.

Reports, before leaving a sensor site, in order to be transmitted to a multiprocessor node's I/O module, go through the modules of the interface unit.

The operation of this interface unit is controlled by a single board computer (SBC). This computer has a copy of the global clock that is synchronized periodically by the control module of the multiprocessor node the sensor is attached to.

a. Analog to Digital (A/D) Converter

It converts the analog report signal as it comes from the sensor into digital (bit string of a fixed length).

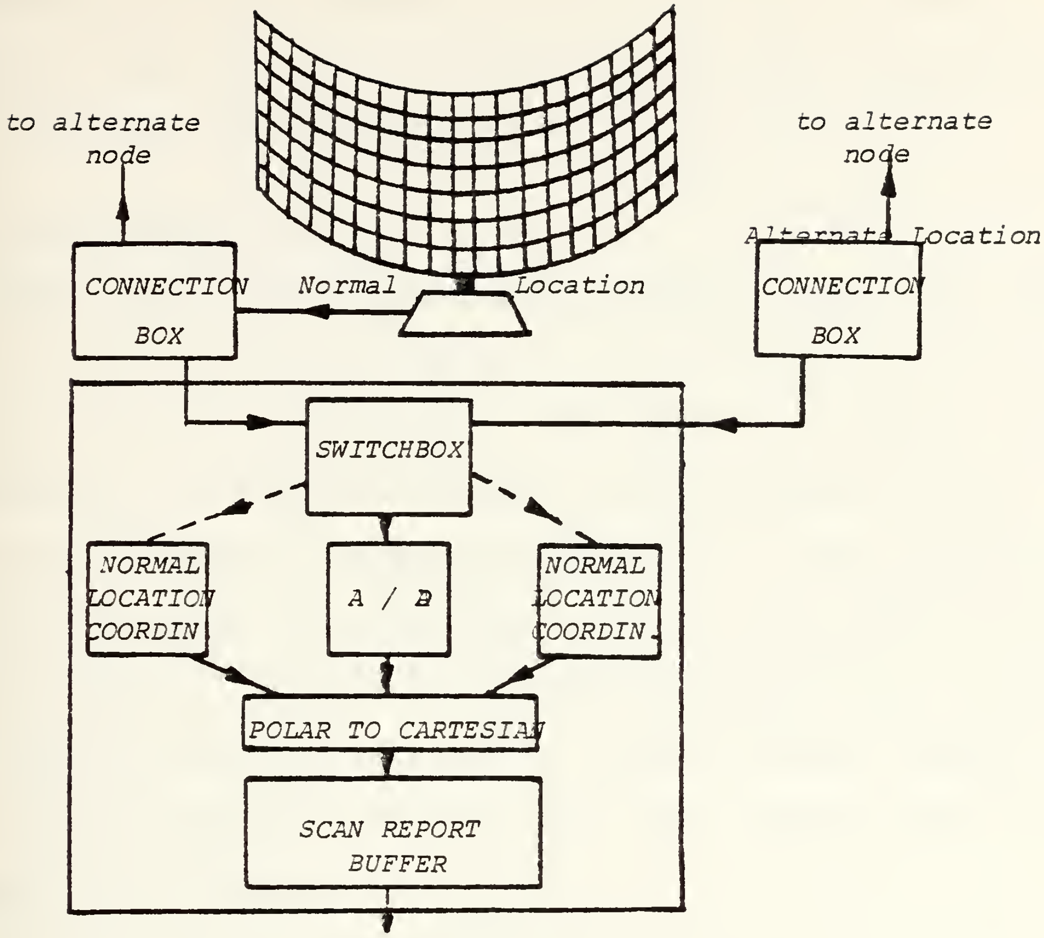


Figure II-7. Sensor Connection to Network.

b. Polar to Cartesian

This unit takes as inputs the digitized reports and the digitally expressed coordinates of the detection sensor's location (normal or alternate) and converts them into cartesian in reference to the global coordinate system.

c. Scan Report Buffer

All report coordinates are loaded into a buffer after the global time component is added to them, in a sequential fashion. The global clock of the system causes the

transmission of the contents of this buffer to the multiprocessor node every "T" seconds, where "T" is the duration of a scan period of the sensor.

C. MULTICOMPUTER NODES

Every one of the multiprocessor nodes has its own computing and data storage potential. In this way, it is able to fulfill all C3 functions within the subarea it serves. Node independence is achieved through the distribution of the processes necessary for data manipulation. Since any one of the multiprocessor nodes may be called to take over the control of sensors lying in its neighboring subarea(s), processes for handling data of all kinds of sensors/weapons systems are distributed there (even if their host subarea does not contain these sensors).

In each one of the multiprocessor nodes there exists a module complex which controls the operation of the other mocule complexes and also synchronizes the node's operation with the other nodes on the network.

Each sensor/weapon system's group has its own dedicated module complex. All interfacing and data association functions for the group is performed within this module complex. Additional module complexes are dedicated to the cross-correlation of data coming from more than one sensor/weapons system's module complexes (e.g. radar/sonar data correlation).

A so called shared local memory holds all information on enemy, friendly and neutral activity within the subarea, plus information of global concern to the system.

The arrangement of the module groups of a multiprocessor node is illustrated in Figure II-8.

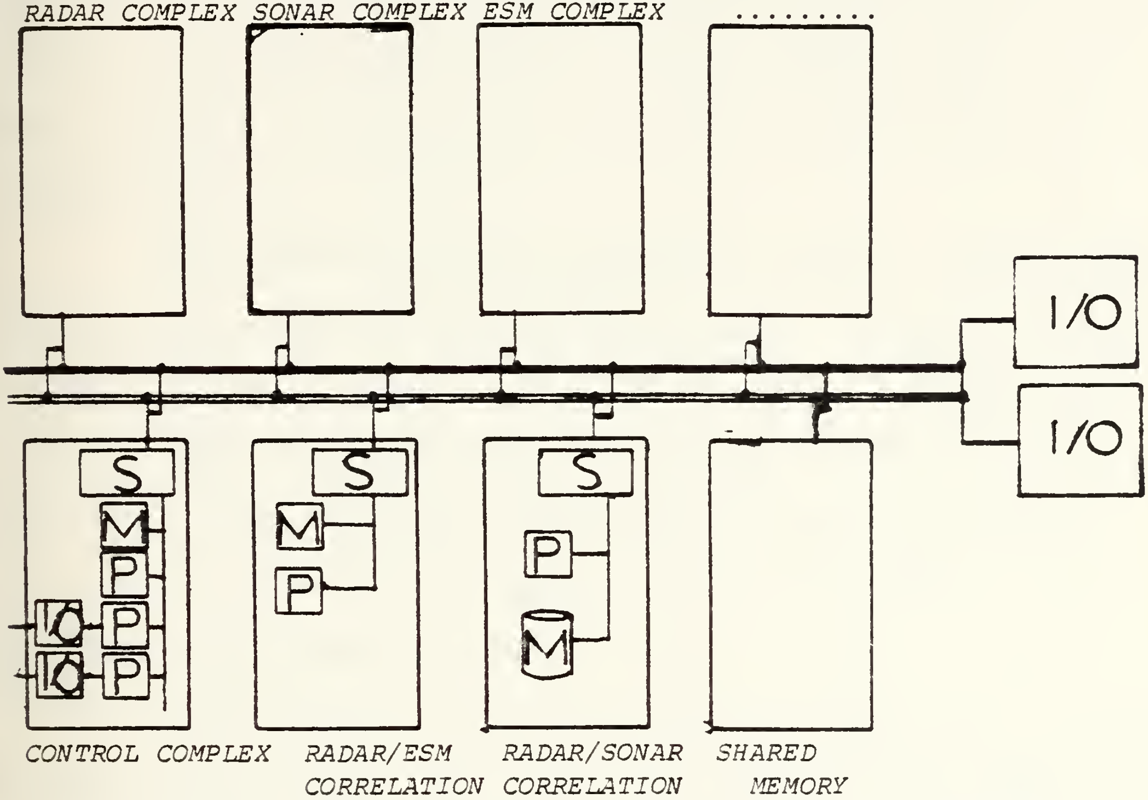


Figure II-8. Multiprocessor Module Group Arrangement.

One of the I/O modules of the node is used for internode communication (fiber-optic interface) and the other to interface with the users in the node environment (consoles, switches, displays, etc.).

The bus which links all the module complexes is a parallel 16 bit one.

1. Single Board Computers (SBC)

A great variety of commercially available SBCs can be used as processors to perform the functions of the modules of the multiprocessor node's complex. An example is Intel's iSBC 86/12, which is low priced ($2000.00 approximately) and offers a flexible architecture. These features make it a very attractive choice for use in the modules of the C3 system.

The iSBC 86/12A is a complete computer system implemented on a single printed circuit board. It has resident a CPU, read/write memory, read only memory, I/O ports and drivers, serial communications interface, interval timer, interrupt controller, and bus control logic and drivers. The central processor for the system is the 8086A 16 bit microprocessor (made by Intel).

These iSBCs can be connected to a common bus in great numbers (10 to 20). They all have their private memory (64K of 16 bit words read/write), while they can access a shared RAM memory of 1M connected to the shared bus. Various combinations of sharing parts or the whole of this memory can be achieved.

2. System's Bus

Within each one of the sensor/weapons sytem's mocule group a number of iSBCs is connected to a parallel bus which has an attached shared memory unit.

As an example, the "Radar Network's Module Group" is as in Figure II-9.

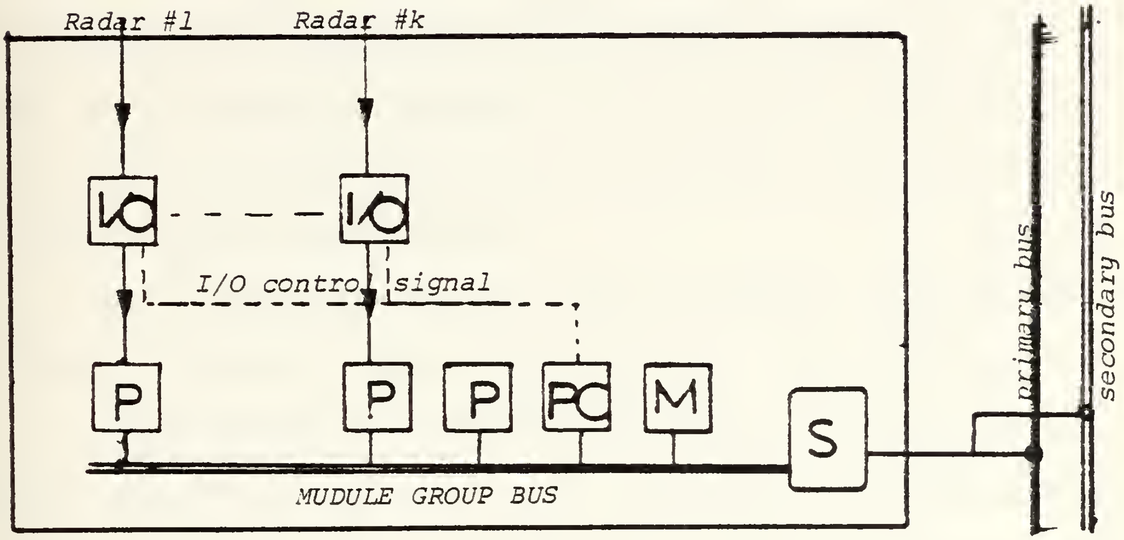


Figure II-9. Radar Module Complex.

Every module group is connected through a common "bus switch" to the parallel multiprocessor node's bus. This switch regulates the I/O traffic to the bus and switches to the standby bus whenever the primary fails (receiving instructions from a Scheduler module).

For each radar for the subarea and for the radars of the neighboring subareas which are alternatively controlled by the multiprocessor node, there exists a SBC. It receives the digitized signal as it comes from the interface unit

through the fiber-optic cable. To switch from the primary to the alternative sensor site line, it has a single switching mechanism which selects one of two existing I/O ports. Input consists of radar contacts (report/time records) as they are described in Section "B" of this chapter. Their output to the processor module (P) are records representing radar contact reports (cartesian coordinates and real time in hours, minutes and seconds).

The processors (P) are used to execute certain correlation processes. These processors are iSBCs 80/86.

Since there is always a possibility that a certain radar's sector is overloaded with contacts (scan report buffer overflow), there exists a mechanism to route excessive reports to a standby processor.

The unloading of the scan report buffers of all the interface units of the radars is synchronized by the module complex controlling processor (PC). This processor sends clock synchronization messages to the radar interface units every five scan periods. It also sends to all the iSBCs of the group a special signal every "T" seconds (scan period). This causes them to start a new surveillance cycle (it is implied that all radars of the radar network must have the same scan period).

The shared memory of the radar module complex holds all active track data in record form. It also holds information

on the utilization of the bus and the protocols used for dialogs among the different module complexes.

The control processor is a dedicated one. It is used to synchronize the operation of the whole complex by operating event-counts based on the scan period of the radars. It also controls the bus switch module (in/out) whenever there is information to be routed to another module complex or to the local memory. This module exchanges synchronization messages with the control module complex to harmonize the multiprocessor node's operation.

D. FIBER-OPTIC RING INTERFACE

1. Description

The four subarea multiprocessor nodes and the two copies of the Global Data Base (GDB) are linked on a delay insertion ring network. The cabling, as it has been stated at the beginning of this chapter, consists of two (distinct geographic paths) fiber-optic channels. Under the geographical topology of the C3 system's network, these two rings will each have an approximate length of 2,000 miles. Point-to-point fiber-optic communications channels are in operation today over distances close to 1000 miles [Refs. 15 and 16]. A Bell Company project has started laying telephone fiber-optic channels between the United States and Europe (PCM system) [Ref. 18].

The bit rate-distance achievable by the commercially available 1.3 μm fiber configuration go up to 500M/sec [Ref. 14]. The signal loss experienced with the latest versions of this fiber is 0.5 db per Km [Ref. 11]. This permits the installation of repeaters every 20 Kms along the ring without substantial signal strength losses. Their bit error rate is less than 5 X 10^{-12}. Bell reports for the PCM system a mean time between failures (MTBF) on its cable of 1 million hours.

The composite cable design is such that a physical protection is provided around the fiber-optic cable for both bend avoidance and physical damage [Ref. 19]. Inside the same coating, the power cables that are used for operating the repeaters, can be hosted as well. Recently, such an underwater working installation was reported as having excellent performance in Tokuyama bay in Japan between offshore petroleum plants [Ref. 20]. Bell for the PCM system specifies these power supply needs for the repeaters as 4 Watts (15 Volts).

Only six interface units are required for the conceptual model system described here (4 for the multiprocessor nodes and 2 for the copies of the GDB). Twenty to forty interface units have been already used in some fiber-optic channel applications. These network interface units have reached performances of up to 100 Mbits/sec at great ranges (600 Kms).

The effect of radiation on the different kinds of fiber cables have been tested at the Naval Research Laboratory (NRL) [Ref. 21]. A great variety of cables produced by various manufacturers were considered. Some test results follow.

ITT (T-323), Polymar Glass Silica
Radiation Dose : 10^5 Rads - Si
Loss : 15 db/Km

Bell (SiO_2 -GeO_2 -P_2O_5 core), Doped Silica
Radiation Dose : 10^2 Rads - Si
Loss : 7 db/Km

Schott (SiO_2 -GeO_2 -B_2O_3 -P_2O_5 -Sb_2O_3), Doped Silica
Radiation Dose : 10^2 Rads - Si
Loss : 1.1 db/Km

In terms of cost, prices vary from less than \$100 to few thousand dollars per Km. Even if some applications would require an investment of \$0.046 per fiber meter, the prices for reliable military systems are much higher. Table II-1 gives a good comparison of cost between metallic and fiber-optic Links satisfying military communications specifications.

The network described in this thesis proposes the use of a 1.3 μm fiber cable with repeaters placed 10 Kms apart and a bit rate of 10Mb/sec.

The operating characteristics of the Delay Insertion Ring network used for the model C3 system are described below [Ref. 10] and the network unit is illustrated in Figure II-10.

TABLE II-1

METALLIC CABLE LINKS VERSUS FIBER-OPTIC LINKS

[Ref. 11]

item	CX - 11230		Fiber-Optic	
Range	8 Km	64 Km	8 Km	64 Km
Data Rate	19.6 Mb/s	2.3 Mb/s	19.6 Mb/s	2.3 Mb/s
Repeaters	19	39	0	7
Cable Cost	$7,000	$56,000	$9,000	$72,000
Rept. Cost	$15,000	$36,000	0	$5,600
Total Cost	$22,000	$92,000	$9,000	$77,000
Syst. Weight	1100 Kg	8700 Kg	280 Kg	1900 Kg

a. Message transmission takes place in the form of blocks of data called frames. These frames are first loaded into the Transmission Shift Register (TSR) and then their routing starts.

b. A destination address is included in each frame.

c. Traffic on the channel is unidirectional.

d. A local Network (node) interface receiving a frame, checks its addressees and if its address is not included, immediately retransmits it back onto the loop. If the node's address is found, it keeps a copy of the message (frame) and makes this fact known by changing a so called "accept" bit in the frame's bit string.

e. The originator node verifies message correctness and the fact that it has been received through the accept bit's state when it comes back to its interface unit (after completing one full loop). If so, it removes the whole message from the channel.

f. The interface unit contains a three position switch (1:FREE_TO_PASS, 2:TRANSMIT, 3:FREE_RSR). The mechanism is shown in Figure II-10 [Ref. 10]. One interface unit exists in every node in addition to one unit for each copy of the Global Data Base (3N/2 units in total for a system with "n" nodes. Odd nodes are truncated to the lower even digit).

g. The length of a frame (in bytes) is fixed. Messages are broken into frames of fixed length in order to be transmitted. The length of the frame equals the length of the Receiver Shift Register (RSR).

2. Fault Tolerance

There are several cases where faults may occur during the operation of the network. The most important of them are mentioned below. Others may exist which are not discussed here.

a. Global Data base Breakdown

In case one of the GDB copies becomes inoperative, the other GDB senses its status through a special message. Then, this other GDB takes over the processing of all multiprocessor nodes requests. When the inoperative GDB becomes

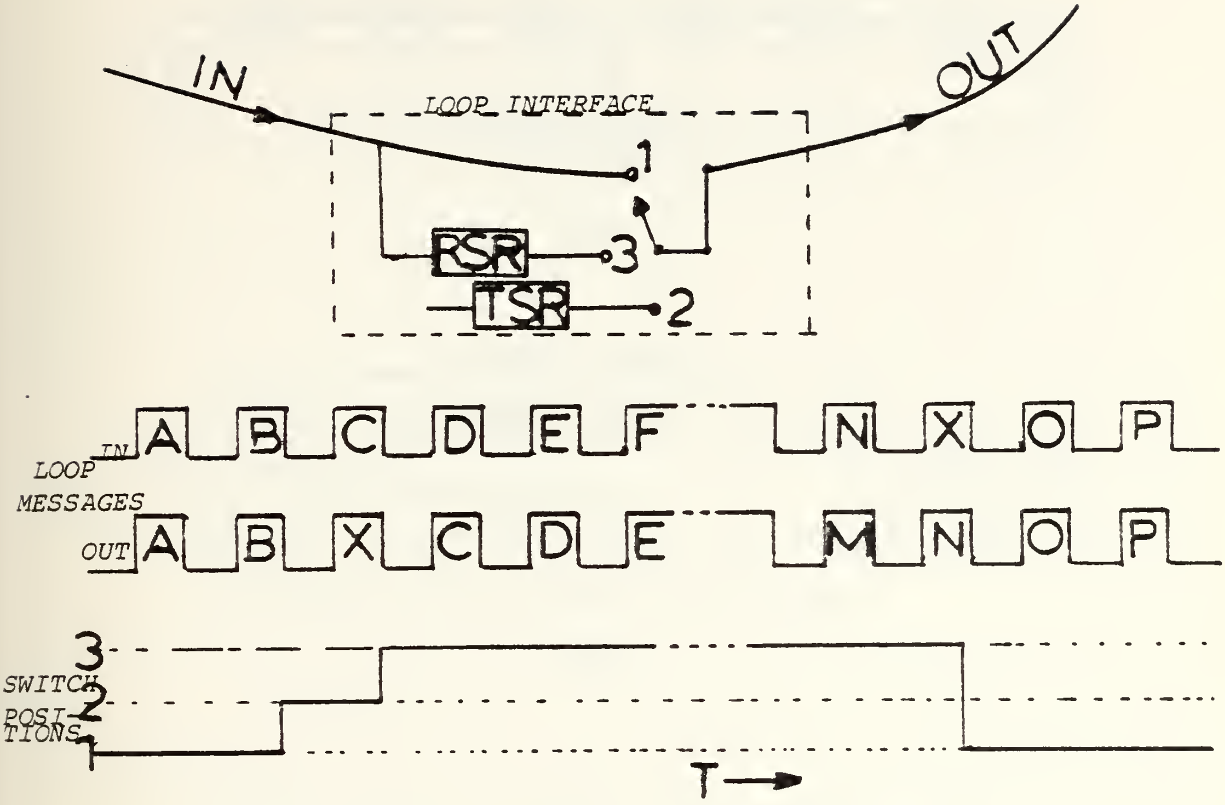


Figure II-10. Loop Interface Operation.

operational again all changes that have meanwhile been made to the other copy are transmitted there. This is taken care of by a mechanism which creates a list of all record addresses that have been accessed after the occurrence of the failure.

b. Network Interface Breakdown

The standby channel is used to close the loop. The architecture used is the one proposed in [Ref. 13] (Figure II-11). This architecture provides for a switch in each one of the interface units to the network which closes

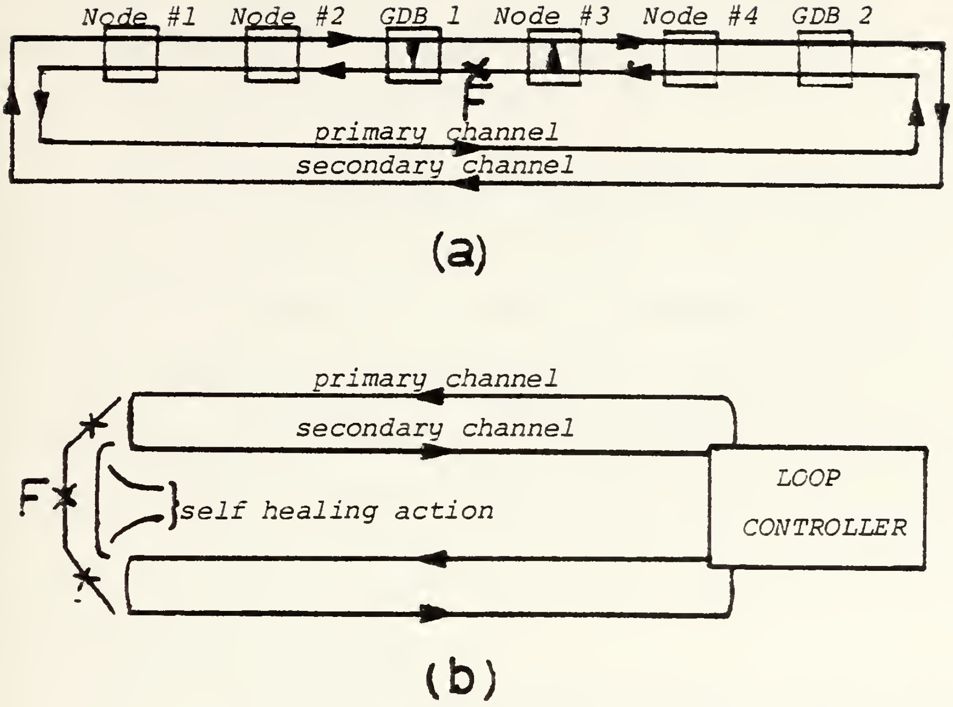


Figure II-11. Standby Channel Mechanism.

the transmission route with the standby channel and forces the legs of both the primary and standby channels, which lead to the failed node, to idle. This, of course, has as a result the reduction of data transmission speed over the network (reduction of the responsiveness of the system). When the neighboring nodes sense this change by the reception of a special message transmitted just before the failed multiprocessor node goes silent, immediately take over the control of the inoperative subarea's sensors via the alternative control lines. When the site recovers, the control of these

sensors is taken back by their mother node. The local data base is updated as necessary. Closing the gap when two consecutive nodes fail, is impossible.

c. Channel Failure

The first multiprocessor node's control module which detects no traffic on the channel for a preestablished time period "Tc" transmits a special message on the primary channel declaring that it switches to the standby one. Then it starts sending its traffic. As soon as the other nodes receive this special message they also switch to the standby channel.

d. System Partition

It is the division of the network into two or more parts. It can happen when a node or both the primary and the standby channel are damaged. In this case the system will operate as a group of separate surveillance systems (the best case being when in every partition a GDB is included). T. Minoura and G. Wiederhold [Ref. 43] have introduced the scheme of a resilient extended true-copy token for distributed data bases. This scheme supports system partitioning without any consistency problem. It is based on a precise treatment of logical data.

A major fault is the breakdown of both GDBs. In this case a gap in the sequence of events is suffered by the system.

III. DATA STORAGE AND DATA FLOW BETWEEN NODES IN THE NETWORK OF THE C3 SYSTEM

A. GENERAL

This chapter refers to the surveillance portion of the conceptual model C3 system. Its objectives are to define data and data organization, to describe the storage models used, and to analyze data flow under both normal and abnormal system's operation.

Data can be categorized into two broad groups: (1) dynamic data (volatile) and (2) static data (nonvolatile). A better understanding of these categories as they pertain to this system can be achieved through the following definitions:

> GLOBAL DATA. All data residing in the Global Data base of the surveillance system.
>
> DYNAMIC DATA. Includes data on targets or other entities that at any one time are within the limits of the surveillance area (or are about to enter) and are part of the current operational scenario.
>
> SUBAREA DATA. It is a subset of the dynamic data referring to the subarea level (the union of the SUBAREA DATA of all subareas equals the dynamic data in the system).
>
> STATIC DATA. Is the complement of the set of dynamic data in the GDB.

The above categorization of data becomes necessary because of their difference in volatility as they are sensed by the system. In other words, a surface or air vehicle subject to continuous tracking has volatile geolocation elements. On the other hand, entities which belong to the static data

category, even if they may be moving, do not have high volatile components and the reports on them received by the surveillance system are occasional or arrive in the form of intelligence summaries (Long Range Maritime Patrol Aircraft, agents, etc.) which refer to long time spans.

Until a so called track of a given contact, which lies within the detection limits of the system's sensors, can be established and associated with a ship/aircraft type, all that is known is a succession of locations (x, y, z coordinate triples). This necessitates the existence of a special data structure called "TRACK" which includes a sequence of at least three location reports followed by their corresponding times. A track is generally characterized as dynamic data.

It is important that the manipulation of dynamic data be performed in real-time, so that the risk of suffering a surprise attack is eliminated. The reduction of the amount of data considered as dynamic allows for fast access (since the data can fit into a fast accessed memory arrangement).

On the other hand, greater delays can be followed in retrieving static data from a much larger storage media without serious effects on the responsiveness of the system. As it will be shown further in this chapter, only a data base can satisfy the needs of storing the static data of the system. The local data for the subarea is at any time resident at the local memory of the multiprocessor nodes.

No special software for the manipulation of the data elements of the data base is included. It is assumed that such a software package already exists. It can be found in the open literature [Ref. 15]. The structure of the conceptual data (illustrated in Appendix A) allows the implementation of such a fast executable software which performs the basic data base functions (get, delete, update, add, create). The choice is left to the implementor and depends on the language his particular computer facility supports.

B. STATIC DATA

Static data is characterized as any piece of information which is not volatile or has a low volatility. For the conceptual surveillance system of this thesis static information includes all the types of data listed below. Their structure is also found in the illustrations of Appendix A.

1. Data Categories

a. Type of Platform

Every radar report is generated by a particular platform type. A type can be aircraft carrier, cruiser, destroyer, submarine or it can be a fighter or transport aircraft, helicopter, merchant ship (oiler, cargo, passenger), commercial aircraft, etc.

b. Class

The class of a platform of type "X" is important to be known as well. The class must also include information on the nationality of the type.

c. Sensor

All sensors (passive/active) that are known to exist in the real world are included into the knowledge base of the surveillance system. Priority is given to the sensors used by the armed forces of the nations of primary interest. Under "sensor" a variety of data structures can exist because the characteristics of a radar, for instance, are different from the ones of a sonar. In addition, sensors are related to sites or platforms they are most frequently mounted on (shore installations or ships/aircraft).

d. Weapon

Similar to the above sensor characteristics also apply to all known types of weapons. Information on the capabilities of the weapon is of great importance to the decision-maker who depends on the surveillance system.

e. Naval Base (or Port)

The position, country, name, ships in port, facilities, defenses, and the operational status of all Naval bases in the area of interest (in a broad sense) are needed in performing geoplot data associations.

f. Airfield (or Airport)

Having information on the airfields helps to determine the nature of the air threat (squadrons, types of aircraft in each airfield, primary mission(s), etc.)

g. Plot

It is almost impossible to keep all the geolocation history of each individual track. By keeping files of tactical plots in a data base it is possible to investigate some incidents and analyze scenarios to derive useful information at a later time. The information that is included in these plot files is the time period covered, area, unit geoplot information (time/position pair groups for each platform), and other miscellaneous information.

h. Meteorological Data

Past, present and predicted information on the meteorological conditions are very useful to the decisionmaker whenever he is willing to dispatch units and assign missions. The information included is sea state, wind, cloud coverage and type, temperatures, humidity, visibility, etc.

i. Hydrographic Data

This is similar to the meteorological information. Hydrographic and sound propagation data (past, present and predicted) are vital to the conduct of ASW and amphibious operations.

j. ROE

The insertion of the rules of engagement into the knowledge bank of the surveillance system permits the High Command to impose its will at any time by simply relaxing or restricting the use of weapons or tactics during the various stages of conflict escalation. These restrictions

are advisory but the knowledge of the ROEs frees the decision-maker from the uncertainty of the political implications of his actions.

k. Country

It is important to know the elements of the military and military related potential each country of interest has. All ships, aircraft types, merchant ship/aircraft companies and airfields, airports as well as ports and naval bases that belong to countries of interest are included.

l. Company

This entity refers to shipping and airline companies. All merchant ships and commercial aircraft of a given country are related to a company. A decision-maker better judges and evaluates information by having access to such information.

m. Platform

A platform is any mobile vehicle which carries a sensor or a weapon. It can be a ship, aircraft, submarine or land vehicle.

n. Site

This data structure includes the coordinates of each one of the shore sites known to have a weapon launching capability or are used as mounts for sensors.

o. Missile

The operational characteristics, the identity signatures (electromagnetic, infrared, optical, acoustical)

and the country each one of the known missile types belongs to are considered as vital information. That information is to be of immediate reach to the surveillance system because of the imminent threat a missile may present to the friendly forces.

2. Data Relationships

The next very important step in the identification of the data structures used by the system is the definition of the set of their interrelationships. The optimization of data association schemas will have as a result savings in both storage space and seek time. It will also simplify the transformation of the information into a storage model and the formulation of the data base(s).

One of the important things in defining these relationships is to allow some room for possible future changes in the data structures (flexibility). For instance, should an extra component become necessary to be added, some of the relationships may have to be redefined.

3. Storage Requirements

Static data has a large storage requirement. Its volume depends on the extent of coverage of the surveillance system. For example, in order to record the military potential of the Soviet Union (types, classes, sensors, weapons systems, etc.), the storage requirements would be in the region of 10^{-8} bytes. The addition of information on other countries and the inclusion of plot, meteorological,

hydrographic and track information for the surveillance area (as analyzed above), increases the storage requirements close to 10^{-10} bytes (once the sensor/weapons systems lists of the 3-4 major manufacturing countries is inserted to the data base, the rest of the countries will occupy relatively small space because these same sensors/weapons are used for platform constructions in different combinations). The above data storage potential is also sufficient for storing extra information concerning the whole Command and Control system.

Only a data base organization (supported by a DBMS) is able to permit efficient access to such a large volume of data within a reasonable time (relative to the needs of military real-time surveillance system).

This so called global data base (GDB) resides in a separate node of the network and has its own interface unit. The GDB is made redundant with the creation of a second copy which acts as backup and shares the transaction satisfaction load with its twin sibling. The physical locations of these two copies of the GDB are so that they reside in every second multiprocessor node. The above architecture offers the following advantages:

a. Increases the throughput on the network since inter multiprocessor and processor/data base transactions can be going on simultaneously on different parts of the network.

b. Reduces the duration of a data base transaction (system's responsiveness) since each one of the GDB copies satisfies two multiprocessor nodes requirements.

c. Increases the survivability of the system in case one of the GDBs fails.

The extra price paid is the cost of 2 extra interface units to the network (one for each of these FDBs).

An alternative that has been considered is to distribute a copy of the GDB to every subarea node. This idea was rejected, first because of the higher cost involved, but mostly because in order to refresh the GDB copy of a failed and later recovered node would block its interface unit for a considerable time, practically prolonging the existence of a time gap in the operation of the system.

The nature of most of the data residing into the GDB is static and as such they are basically loaded manually or through interface modules to other information systems.

In one of the sites, where a copy of the GDB is hosted (primary GDB), there exists a so called "GDB Custodian Facility". This facility consists of a number of people, terminals, and a repertoire of applications programs. The GDB Custodian Facility collects information from various sources, as is shown in Figure III-1. This way, the static data of the GDB is kept updated. Its operation is similar to that of an intelligence agency, where information has to be filtered, correlated and assigned a "confidence level". When the confidence level of a given information chunk exceeds a preestablished threshold value, the information is used to update the GDB.

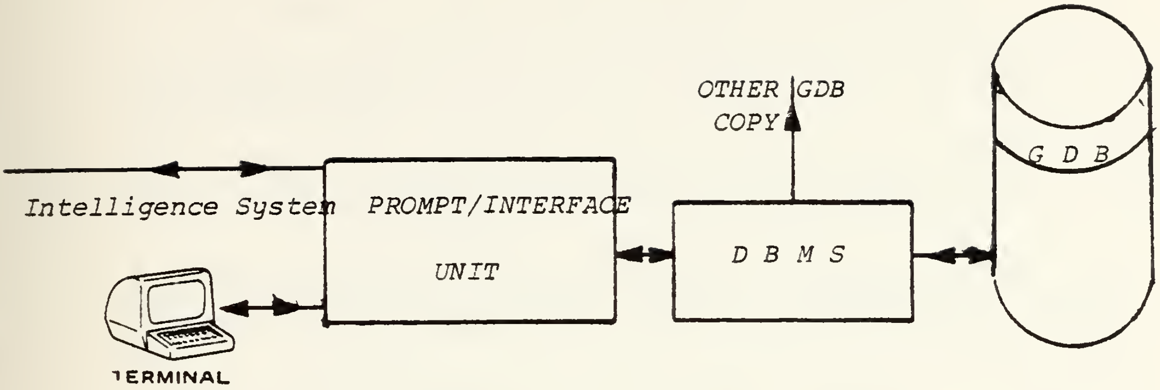


Figure III-1. GDB Custodian Facility Operation.

To ensure that all necessary components of an information chunk have been included during the GDB update, the application programs have been made interactive. Given the type of data being updated, a sequence of prompt questions are posed to the updating personnel.

The priority in satisfying transactions by the GDB Management System is as follows:

a. Retrieve transactions from subarea sites.
b. Update transactions from subarea sites.
c. Update transactions to the subarea sites.
d. Update transactions made by the GDB Custodian Facility.

The above priorities are established to ensure that the most urgent work is done first and the system performs in real-time. A number of buffers (spoolers) is used to withhold waiting transactions before they are introduced to the DBMS.

When a target detection report is entered to the GDB via the Custodian Facility (Long Range Maritime Patrol Aircraft, intelligence, etc.) the following happens:

a. It is determined near which subarea(s) the target's position lies.

b. The report is routed to this subarea's multiprocessor node (to be entered into the local memory).

c. A search is performed in the GDB based on existing relations and all related report information is retrieved to be sent to the multiprocessor node concerned.

The same procedure is followed whenever a target is first detected by the sensor of a subarea and this initial report is sent to the GDB. Of course, in this case some extra data are needed in order that the target be identified. Figure III-2 illustrates the above process.

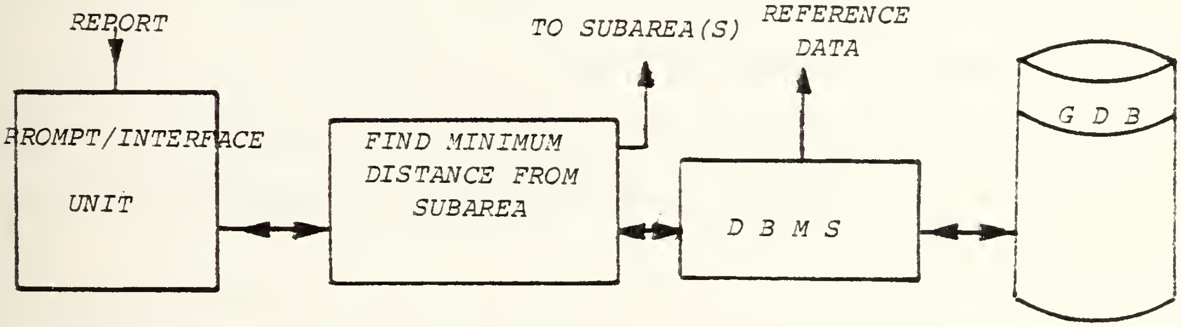


Figure III-2. New Report Data in GDB.

4. Response Times

A good organization of the data and their relationships in the data base (relational data base) is estimated that will permit an average of 50 milliseconds access time. This number includes also the communications delay (due to the length of the fiber-optic cable) and assumes an average traffic load on the ring network [Ref. 10].

Based on that response time, the following rough calculations can be made to find the throughput of the network:

Single Transaction Response Time : 50 msec
Number of Transactions per Second : 20
Number of Transactions per Scan Period : 120/6sec

Global Data base Update (every 30 scan periods)
30 X 120 = 3,600 transactions

The number of 3,600 GDB transactions that can be performed per GDB update includes both routine and nonroutine transactions. Routine transactions are record updates. Nonroutine transactions take place in the cases of first detections, track initializations and imminent threat reports. The above throughput is considered as adequate for any practical requirements of the proposed C3 system.

C. DYNAMIC DATA

All information that is related to the scenario in progress in the surveillance area is called dynamic. Local data is a subset of the dynamic data and refers to an individual subarea. Dynamic data is of two types, reference data and tracks/reports on platforms.

Reference data is static data that must be available in the local memory of a multiprocessor node so as to enable it in carrying out its identification and classification functions.

Track/report data form a separate data structure type which is described later in this section.

1. Reference Data

For each track which has been identified to belong to a specific platform, all information about the type, class, sensors/weapons systems it is equipped with, and its home-port are included in the reference data set. Meteorological and hydrographic data referring to the present and predicted conditions as well as the immediately previous and current plots for the subarea are also included. The above information is supplemented with data on imminent threat platforms (e.g. when a specific fire control radar (FCR) is intercepted, it gives the indication that an enemy missile is about to be launched). Finally, the rules of engagement (ROE) in effect at any time constitute part of the reference data.

Reference data insure the subarea Commander's independence and make the response of the system as a whole more rapid. The mechanisms which are used for updating the reference data set (additions/deletions) of each individual multiprocessor node have been described in the previous section.

2. Tracks/Reports

A track is a data structure which has at least the following components:

a. Two or more positions (x, y coordinates) together with reference times (two locations only when the positions are a result of a visual identification).

b. Track number (as in Chapter IV, Section E).

In addition, the inclusion of the following components into the structure of a track are considered as helpful in increasing the responsiveness of the surveillance system.

c. Heading derived from consecutive locations.

d. Speed calculated on the basis of locations and their corresponding times (can be analyzed into three subcomponents in the directions of the principal coordinate system's axes).

e. Size of contact, as it is sensed by the detecting sensor.

f. Type of target, such as cruiser, submarine, helo, fighter aircraft, etc.

g. Plot the track is related to.

The values of the components (c) through (g) are not necessarily always known. It becomes clear at this stage that whatever relation is to be established between a track and the GDB, it must be based on positional data (including time).

A report is a special case of a track. It includes only one positional component and a "track-no". Depending on the type of the detecting sensor, it may or may not include the rest of the components of a track. For reasons

of simplicity, a report is handled by this system as a track with null values assigned to some of its components. Figure III-3 shows the structure of a typical track record as it is conceptualized above. An extra field is reserved for linking purposes (next).

tr_no	t1	t2	t3	ps1	ps2	ps3	size	heading	speed	type	plot	next

Figure III-3. Track Record Structure.

A typical relationship of a track is discussed below.

TRACK - PLOT.

Starting from the moment one of the surveillance system's sensors locates and starts tracking a given target, the following questions demand an answer:

a. How can the track be associated with a type?
b. Where did it come from?
c. What threat does it pose?
d. How is the track related to the general tactical picture?

In order to answer these questions it is necessary to use some of the relationships of the previous section plus the relationship between TRACK and PLOT as shown in Figure III-4.

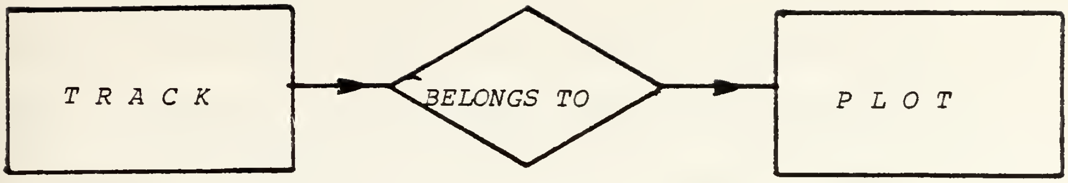


Figure III-4. Relation of TRACK to PLOT.

3. Storage Requirements

The nature of the surveillance system described in this thesis is such that real-time performance is what must be of primary consideration. As a consequence of this, data must be represented, related and organized in the memory in such a way, so to be accessible as fast as possible.

The data structure the system has to do with more frequently is the TRACK (or REPORT). It is important to identify this entity (especially if moving fast). So, elements of the TRACK are used in the formation of an index to the local memory.

The components (or fields) of a track can be separated into two broad categories, the "overt" and "covert" ones. The first are the ones directly sensed by the sensors of the system. They are TIME, LOCATION (x, y, z) and SIZE of return. All the rest are covert and take assigned values or are calculated by the mechanisms of the surveillance system's processing elements.

Generalizing things a little more, it is almost certain that the approximate location of a given TRACK will always be known. If the chosen basis for calculating the key component to address the track record is the location of the track (last sensed position), it is implicit that one of the two coordinate systems used in operations should be chosen.

The cartesian is much more suitable than the polar coordinate system for the network wide coordinate system.

To minimize the average data seek-time and avoid large deviations from this average, a close to uniform distribution of records into the local memory is desirable.

Through a division of the whole area covered by the surveillance system into equal size squares it is possible to distribute the TRACKs according to their location almost uniformly. It must be realized that some squares will be more dense during several "time spans" and some others will have a continuously high density (focal points, such as vicinity to ports and airport terminal areas).

The size of the manageable square area in terms of track capacity and practical handling, as well as the size of the total area which is kept under surveillance by the system, determine which hashing method will be used.

a. Surveillance Area Size

Neither of the x, y dimensions of the surveillance area exceeds the 1000 N.M. Under the coordinate grid addressed

above, every track can be referred through the triple x, y, z where both x and y range from 000 to 999, and z from -3,000 to 100,000 feet for all realistic purposes.

b. Manageable Area

In a modern naval conflict scenario or in a tension period situation (which are the two cases where speed is of great importance) no more than 20 tracks are likely to coexist within a 10 X 10 square miles area extended vertically to the limits defined above.

The above assumptions make the implementation of a hashing function possible, which uses the most significant two digits of the track's x and y coordinates as an index to the hash table.

For example, a track's last location x=217, y=522, z=17300 is expressed as 21, 52. If now these two numbers are concatenated so as to form a 4 digit integer, they can be easily used as an index to a storage block address.

This arrangement facilitates the fast association of a track lying in adjacent squares (they occupy memory locations close to each other in a storage media) and allows for a continuous rearrangement of tracks into blocks as they move in the real three-dimensional space.

This hash function can be implemented in a Pascal-like language. An example is given below.

Function invocation

```
address := hash (x,y);
```

Function declaration

```
function hash (X,Y:real):integer;
    hash := (integer (X)/10)*100 + integer(Y)/10;
end;
```

The total memory capacity requirements for the dynamic data storage is estimated to be in the order of 1Mb. This data can be stored on RAM memory commercially available today.

4. Response Times

The response times that are estimated as achievable by the system for the dynamic data are equal to real-time. This is accomplished by the partitioning of the dynamic data and by distributing the partition elements into the local memories of the multiprocessor nodes. This way, communications delays are eliminated for all practical purposes and the overhead to access dynamic data is minimized. An average data access operation can be completed in less than 1.4 sec (access to the bus and memory I/O). This way, within the 6 seconds of a scan period, a minimum of 4,300,000 memory accesses can be accomplished at the multiprocessor node level.

This number exceeds the needs of the surveillance system and leaves room for comfortably using the shared memory to store other information as well (e.g. correlation processes and other software modules which are loaded for execution to available SBCs of the complex whenever they are invoked).

D. DATA FLOW

The data that flows between the different parts of the system consists of records and special messages. The records represent the data entities described in the previous sections of this chapter. Special messages are used for system control and synchronization.

Data flow on the internode network makes use of the fiber-optic ring structure and consists of frames of data that also contain address(es) and other network control information. Inside the multiprocessor node, data flow between the module groups makes use of a time shared parallel system's bus.

In the following paragraphs the mechanisms used to ensure the fast and reliable flow of data are described both, inside the multiprocessor node and for the internode network.

1. Data Flow on the Network

The information exchange requirements of the subarea nodes govern the flow of data along the network. This flow gives a clear view of how the system operates.

The major advantage of the register insertion ring network, used in this architecture in terms of data flow is that multiple transactions between nodes can be going on simultaneously.

In each node, the data before it enters the Transmit Shift Register (TSR) is converted into "frames" that include some extra control bits and the addresses of the originator

of the frame and its destination. These bits are called the "match" and the "accept" bits. They are part of the overhead which is used to verify that the transmitted data has been properly received by the addressee nodes. The way this is done is described in Table III-1 below.

TABLE III-1

MATCH AND ACCEPT BITS

[Ref. 10: p. 65]

Match bit	Accept bit	Meaning
0	0	The message was addressed to a node that does not exist; no interface unit recognizes the message.
0	1	The message was successfully transmitted to one or more nodes; at least one interface unit recognized the message.
1	0	No node received the message; however, at least one interface unit recognized the address in the message.
1	1	The message was addressed to nodes in at least 2 subareas. At least one interface unit was able to copy it and at least one was unable to copy it.

Both "match" and "accept" bits are initialized to "0". When the frame they are attached to makes a complete circuit on the ring, the RSR of the originator node checks their status and the correctness of the bit string compared to the transmitted one. If the message bit string is found to be correct, the accept/match bits are examined. In case

a 0-1 is found, the originator's interface unit removes the frame from the network. Otherwise, it retransmits the correct message.

Any node interface unit recognizing its address in a frame changes the accept bit into "1" (after successfully copying the carried message). The match bit is changed to "1" by a receiving node whenever a successful copy has not been achieved.

a. GDB to the Multiprocessor Node

The data of the surveillance system which flow from the GDB to a multiprocessor node are records of entities which, either have been requested by the node addressed or have been judged as necessary to be sent to the node(s). This last category of transmitted data is a result of the insertion of new data (static) into the GDB through the GDB Custodian Facility and have as a result a change of the operational scenario. The sequence followed in order to initialize such a transmission is illustrated in Figure III-5.

The GDB node initiating such a transmission is the primary one (the one that has the GDB Custodian Facility).

In satisfying a multiprocessor node's request, the GDB node which as received the request, transmits the requested record to the node (the requestor's address has been kept in the spooler). This mechanism's operation is illustrated in Figure III-6.

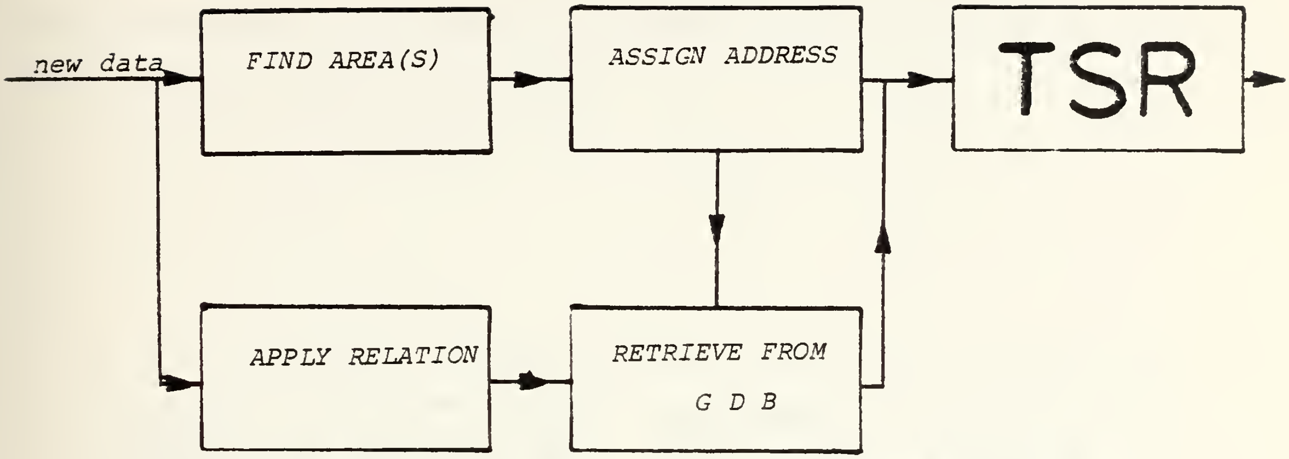


Figure III-5. New Data in the GDB.

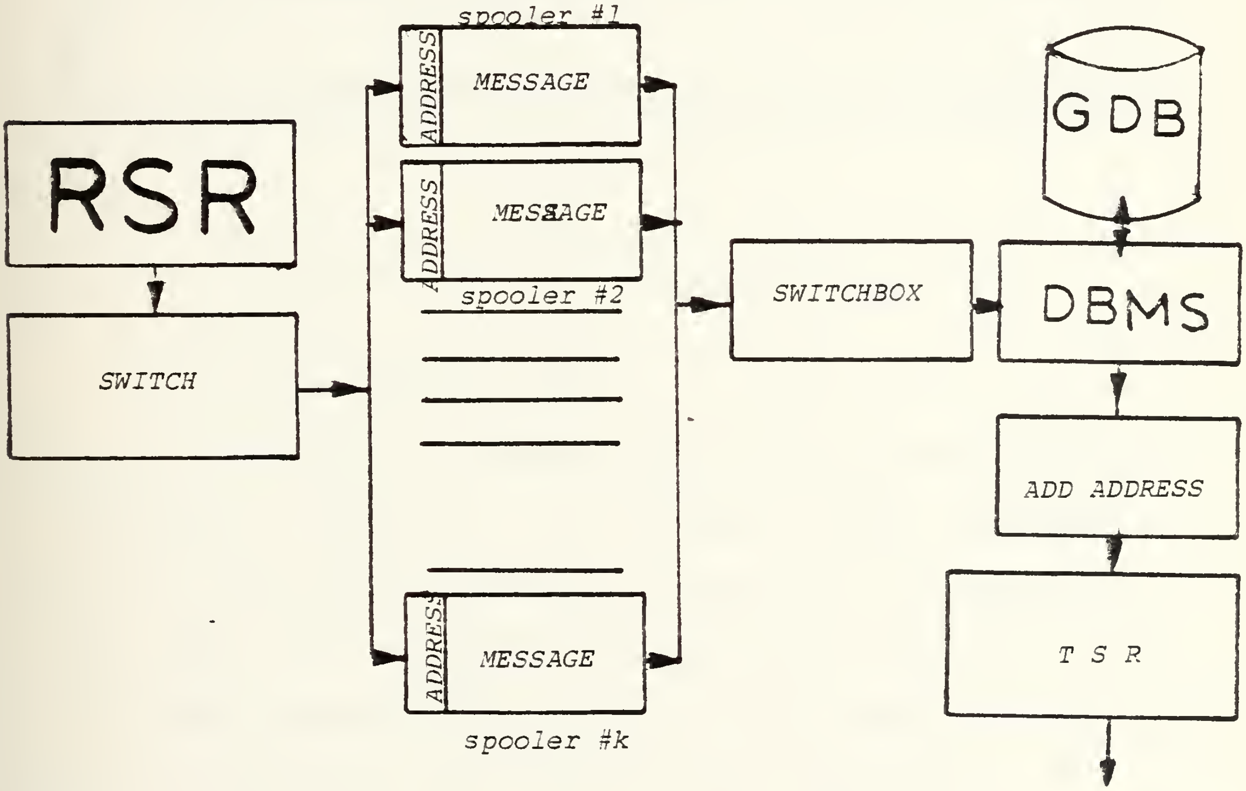


Figure III-6. Request Satisfaction by the GDB.

Normally each GDB copy serves the requests of two multiprocessor nodes (Figure III-7). In this figure, each dot-surrounded box indicates the GDB which collaborates with a pair of multiprocessor nodes.

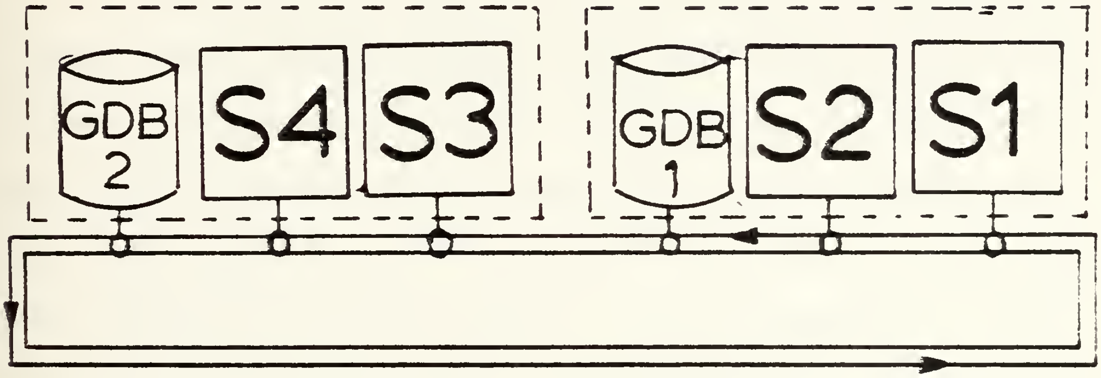


Figure III-7. Collaborating Nodes.

b. From a GDB to a GDB

Such an information flow occurs whenever data is inserted to the primary GDB through the GDB Custodian Facility. All the so inserted information is transmitted to the other copy of the GDB independent of its transaction to any other multiprocessor node(s). This way, the two copies of the global data base are kept identical.

c. Multiprocessor Node to the GDB

The data transmitted from a node to the GDB is of several kinds. First of all, an initial report of an object, detected by a sensor of the subarea, is transmitted to the GDB with a maximum delay of 6 seconds. In addition to this, whenever a track on this object (platform or missile) has been obtained, it is also transmitted to the GDB.

The rest of the data flow (node to GDB) consists of track record update messages which are sent in the form of frames. Since that kind of data are, under normal conditions, vital to the subarea Commander, their transmission to the GDB is done every 5 scan periods (rapid transmission is not necessary for that data). In the meanwhile, data which are to be transmitted by a multiprocessor node during the next transmission are stored in special transmit buffer complex. Figure III-8 illustrates how this mechanism works.

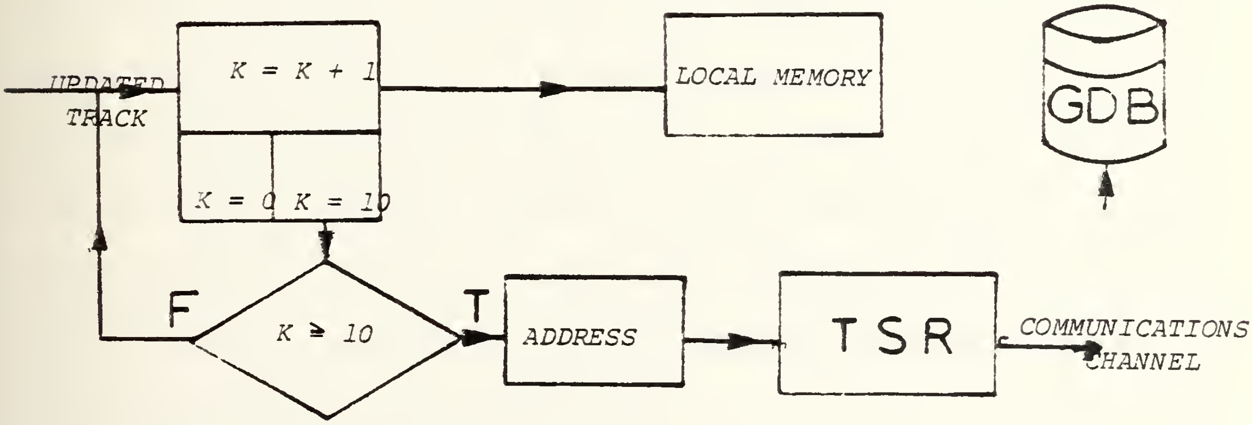


Figure III-8. Global Data Base Update with Dynamic Data.

d. Among Multiprocessor Nodes

The data flow between the system's multiprocessor nodes consist of dynamic data that refers to tracks which have motion going from the transmitting subarea to that of the addressee(s). The criteria used for initiating such transmissions are their vicinity to the boundary line between the two subareas and their heading. These criteria can be altered to include all track data in the subarea whenever the addressee node's subarea Commander is assigned the coordination of the operations within the transmitting node's and his own subarea.

These transmissions are done following the same transmission intervals with the global data base (GDB) updates (every 30 seconds).

2. Data Flow Inside the Multiprocessor Node

All data flows inside the multiprocessor node through the common bus. The difference from the data flow on the network is that for each individual sensor complex the data which flows in and out of its module group is in terms of the records of the data structure it supports. For instance, the Electronic Support Measures (ESM) module group's complex will receive or transmit only active SENSOR records (radars, IFF equipment, jammers, etc.) and REPORTs before and after triangulation has been achieved.

The reference data, as it comes into the multiprocessor node's environment, is loaded to the shared memory of each individual module group (related data only).

Whenever the control module group gives a synchronization message to the different module groups they send their correlated data (track or report records) to the shared memory, and the sensor combination module complexes so the information may be further classified. This does not apply to the initial detection reports which are transmitted directly to the TSR. Data coming from the sensor combination module complexes is loaded into the local memory. In addition it is sent to the transmit buffers of the node's network interface unit. The processor which is attached to the local memory module complex assigns track numbers to the incoming new reports and returns these track numbers to the originating module complex(es).

The description of the inter module complex data flow is omitted from this chapter (it is given in Chapter IV).

The flow of data in the multiprocessor node environment is shown in Figure III-9.

Once in every scan period (6 seconds) data from each one of the sensor module complexes flows towards the Local Memory, the Multisensor Complex (Radar/ESM complex in Figure III-10), the I/O module to the ring interface unit (initial reports only) and the I/O module which serves the human interface facility in the subarea Command post.

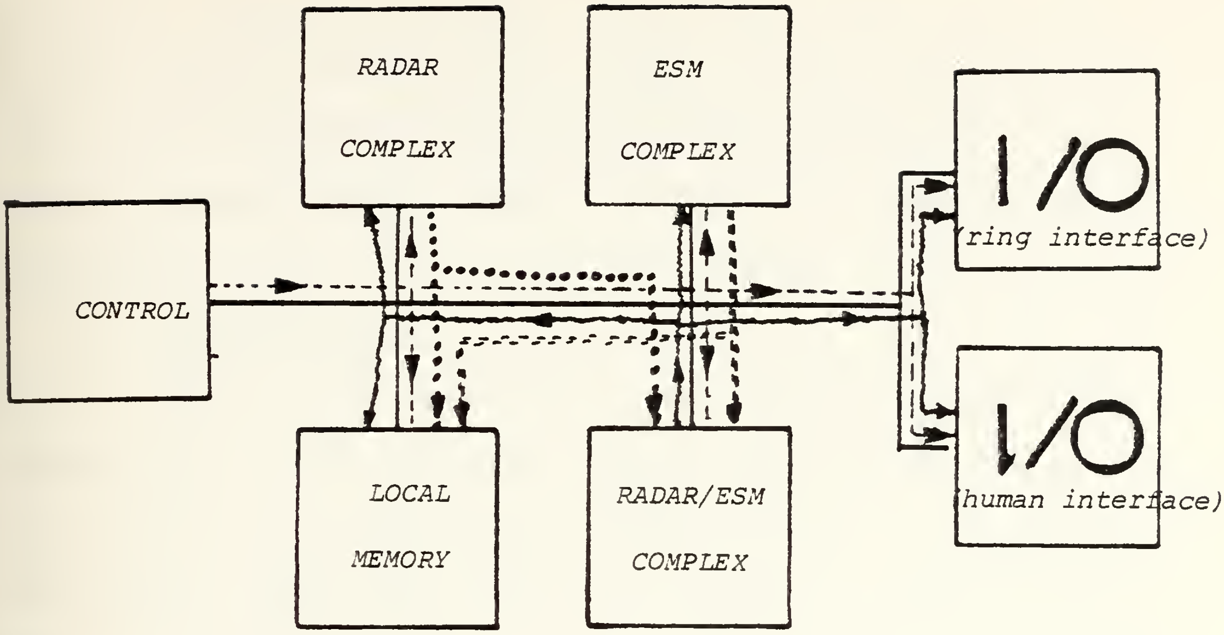


Figure III-9. Data Flow Inside the Multiprocessor Node.

The Radar/ESM complex outputs data for the Local Memory and the Sensor Module complexes, where the derived discrete characteristics of each report or track are added to their records as well as the assigned track number. Just after this complex classifies a track (or report) as hostile, its record is also routed to the I/O modules. This data flow takes place every 6 seconds also.

The Local Memory transmits GDB update data once every 30 scan periods (3 minutes). This transmission is done through the I/O module interfacing the ring.

E. DATA FLOW IN CASE OF FAILURES

The failures which are considered in this section refer to the major components of the distributed surveillance

network. These failures will be examined from the aspect of their effect on the flow of data. Namely, the failures that are addressed in the following paragraphs are link failure, node failure, interface unit failure and system saturation.

1. Link Failure

When a link connecting two different nodes on the channel fails, no traffic is further received by the second node (in the direction data normally flows). This second node detects the link failure by lacking any input on the RSR of its interface unit for ten loop periods. This time is equal to 100 microseconds (which equals the time it takes for a bit to complete ten full loops on a 3,000 Km fiber-optic cable under uninterrupted flow conditions). Both the primary and the secondary GDBs, every one loop delay period transmit a special bit string to indicate that they are still "active" on the network (normally one of these bit strings is received every 5 microseconds). The detecting node assumes that a link failure has occurred prior to it. The control module complex of this subarea's multiprocessor node generates a special message. This message is transmitted on the primary channel and immediately following all data flow originating from this node starts being transmitted through the standby channel.

The rest of the nodes, as soon as they receive this special message (bit string pattern), switch to the standby channel.

With this arrangement no data is lost since a copy of all frames transmitted by any one of the nodes on the network is kept at the originator's transmit buffers until it can be compared with the returning identical frame. This way, no data is lost since the frames can be retransmitted on the standby channel.

When the originally primary channel becomes operational again it acts as a standby channel since there is no difference between the two of them.

2. Node Failure

As it has been defined previously, the nodes can be categorized as GDB nodes and multiprocessor nodes. Each one of these node categories, even if it has a similar interface unit to the network, serves a different purpose. So a failure of a node belonging to one of these categories must be separately discussed. However, some reactions of the network to node failures of both of these categories are similar.

a. GDB Node Failure

Each GDB's node interface unit has an extra mechanism which produces a characteristic 16 bit string and transmits it on the communications channel once in every ten loop delay periods. When this string returns to its originator GDB, a part of it is incremented by 1 and immediately retransmitted. Each GDB has its own characteristic bit string so the status of each one of them can be determined very frequently.

When a node hosting a copy of the GDB fails, it becomes unable to accept requests from the multiprocessor nodes it serves. By being unable to increment its characteristic bit string, it allows the node hosting the other GDB copy to detect the failure. After failure detection, the other copy of the GDB takes over the satisfaction of all node requests. As a consequence, the throughput on the channel is reduced down to the half of the normal. Still, the system is able to operate, since the number of transactions is less than the capacity of the single GDB.

Failed GDB recovery is handled in steps. For all the GDB records that have been updated an address list is kept and only the last update made to the record is stored there. Addresses and records are kept in parallel arrays of address/buffer pairs which are used during the refresh of the recovered GDB. When the last of these buffers is emptied, a message from the refreshing GDB triggers the reactivation of the bit-string incrementing mechanism of the recovered GDB. From this moment the system restarts its normal operation again.

The above GDB failure management procedure is hidden from the multiprocessor nodes which keep addressing their requests to "the GDB" (one address exists for both GDB copies, but their interface units are smart enough to satisfy requests depending on the requestor).

b. Multiprocessor Node Failure

The failure of a multiprocessor node creates a greater problem for the surveillance system because all information on the activity taking place in the subarea it supports is denied to the rest of the system. In this case the interface unit transmits a special message (bit string) on the network channel which announces the inoperativeness of the node.

Adjacent subarea's multiprocessor nodes receiving this message immediately activate their switch boxes which close the alternate connections with the sensors normally controlled by the failed node. This sensor sharing is preagreed and on a 50/50 basis.

In addition to the extra processing load they take, the set of the local data of the failed node is sent to the take-over nodes from the GDB. This, on one hand increases the traffic on the channel, but on the other reduces the complexity of processing at the multiprocessor level (there exists reference data).

The reverse process (node recovery) is simpler since all the necessary local data, as well as the control of the sensors, are passed back in a stepwise fashion.

3. Node Interface Failure

In this case, the same as in the failed node problem handling sequence takes place as for the control of the sensors. The difference lies in the utilization of the

communications channel. Since the interface unit is inoperative, the traffic cannot go through. So the ring loop closes by the special arrangement shown in Figure II-11 with the utilization of the standby channel. In this case a greater communications delay is exercised on all internode transactions because of the cable length increase. This is the minimum price which can be paid.

4. Network Saturation

Network saturation occurs whenever a GDB refresh takes place or when a node which had failed recovers and its SUBAREA DATA is updated. In these cases the data flow on the channel increases substantially and the network becomes saturated. To avoid this kind of saturation, a so called "SLOW/FAST mechanism" counts the length of the transaction queues at the interface unit's receive buffers. When this length exceeds a preestablished threshold value, the node suffering a long queue transmits a "SLOW" message which forces the rate of the dynamic data update to be reduced so that instead of 30 scan periods (which is the standard) it becomes 30+10. This incrementation continues on an n+10 basis up to 60 scan periods (6 minutes) if it is required. When the length of the queues on all nodes starts decreasing, the node which has transmitted the last "SLOW" message starts transmitting a "FAST" message that decrements the number of scan periods corresponding to the system's rate of operation by 10 (the same way) down to the standard of 30 scan periods (3 minutes).

5. Multiprocessor Node Saturation

It is possible for a given surveillance subarea to experience a high target density situation. In this case, if by utilizing the standby processors it hosts, it becomes impossible to satisfy the surveillance requirements in its subarea, another node's contribution is requested.

The procedure followed requires the saturated node to transmit a special "OVERLOAD" message, which indicates that a node is ready to transfer the control of some of its sensors lying close to adjacent subareas. The sequence of transfer is preestablished (e.g. specific radars are listed in an array). This hand-over procedure takes place in steps (layer stripping). When the load at the overloaded multiprocessor node is reduced, a "RELAX" message is transmitted by the node which has originated the OVERLOAD message and the control of its sensors is reassumed in reverse order.

IV. DATA AND PROGRAM ORGANIZATION WITHIN THE COMPUTING NODE

A. PROCESS/TASK ORGANIZATION

Each of the computing nodes of the C3 system has a similar internal process/task organization. Processes specially designed for the manipulation of data of all the sensors/weapons systems do reside into each computing (or processing) node. This enables the nodes to exercise their take-over functions whenever neighboring nodes fail.

In this section only the organization of the processes in the radar module complex will be presented in detail (Figure IV-1). Similar is the structure of the rest of the sensors/weapons systems module complexes with minor differences.

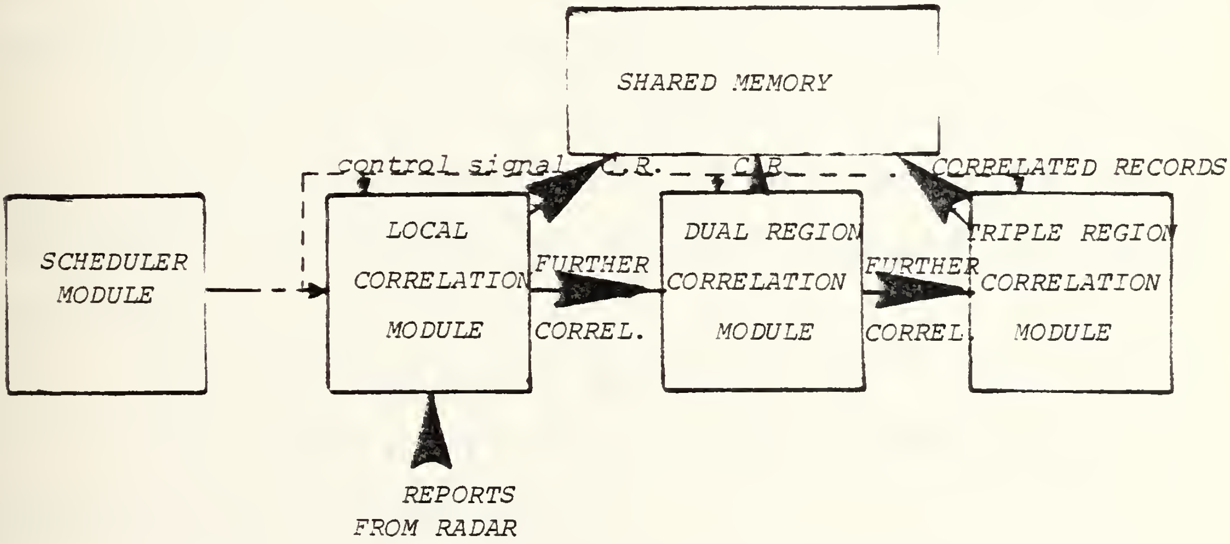


Figure IV-1. Time Sequence of Processes in the Radar Module Complex.

1. Assumptions

The assumptions on which the organization of the processes is based are listed below:

a. All radars are surface search ones with an equal Aerial Rotation Period (ARP) of 6 seconds (otherwise referred to as "scan period"). There is no height finding capability.

b. Radar detection sectors are circular with a radius equal to their maximum detection range. This helps in reducing redundancy and in resolving conflicts in cases where two neighboring radars happen to be tracking the same target.

c. Each individual radar in the subarea can have regions of overlapping sectors with at most 4 neighboring radars. In addition, no more than 3 different radar sectors can overlap over any given region. This assumption is not considered as strictly restrictive to the system. It would be able to function even if 5 or 6 radar sectors where overlapping (with some modifications in the software).

d. The velocities of the targets the system may track are up to 1000 knots. Minor modifications to the software modules would enable the tracking of targets with higher velocities.

e. Target density in the area is 0.007 targets/sq/Km.

f. Targets can be of any of the following types (both military and commercial):

(1) Ships

(2) Helicopters

(3) Submarines

(4) A/C and missiles flying at low altitude.

2. Process Organization

The software modules of the Radar module complex are organized so as to be executed by dedicated and nondedicated single board computers (SBC). A description of each one of these and of the Radar interface processes follows (the SBCs dedicated to the execution of the radar interface modules are physically located at the radar sites instead of at the multiprocessor node).

3. Radar Interface Module (RIM)

Each radar is directly (point-to-point) connected to the radar module complex through an interface unit. Interface units are located close to the radar site. All detection signals (reports) from the radars are transmitted in real-time through wiring to their corresponding interface units. These reports (raw analog data) include the polar coordinates of each radar return (report) and a size value for these returns. The RIM converts the polar coordinates into cartesian (x, y) in Km. In addition, it attaches to this position a time component taken from a copy of the global clock. The report record formed has the following structure:

REPORT (time, x_coord, y_coord, size)

Note: The size of a report is measured on a scale 1 to 3.

All reports, after they have been processed, are loaded into the SCAN REPORT BUFFER. This buffer holds the reports acquired over one scan period (6 seconds).

The initiation of the new scan period is done by the Scheduler module of the Radar module complex through an event_count message.

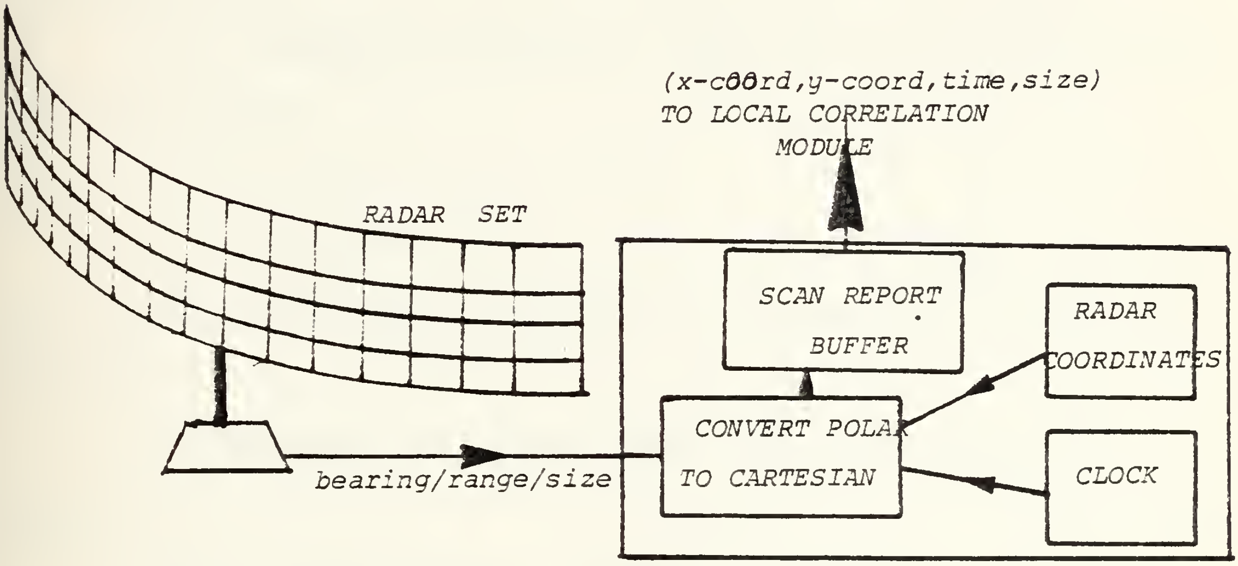


Figure IV-2. Radar Interface Module.

4. Local Correlation Module (LCM)

Each RIM is connected through fiber-optic cable to a SBC at the multiprocessor node's physical location. This SBC is dedicated to the execution of a Local Correlation Module corresponding to its particular radar sector. Every radar sector is divided into four quadrant sectors (000-090,

090-180, etc.). This division is used by the system's overload handling mechanism which will be described later in this chapter. This module every 6 seconds (scan period) reads-in the report data from the RADAR BUFFER of its assigned RIM and does the following:

a. Uses special overload relaxing mechanisms that take over in cases where the number of reports loaded in "X" from the radar buffer at any one scan is greater than 40.

b. Attempts to associate report data with the already existing tracks.

c. Initializes new tracks.

d. Separates the data that belong to tracks which are in the regions where the sector overlaps with other sectors.

e. Updates the shared memory with the remaining data.

Each LCM maintains a number of internal buffers in order to facilitate data manipulation. These are:

a. Buffer "X"

It keeps report data that is read from the SCAN REPORT BUFFER of the RIM.

b. Unresolved Reports Buffer "T"

It holds the report data which has not been associated with any track, or has not been used to initialize a track for six consecutive scan periods (36 seconds).

c. Temporary Track Pool "TPOOL"

It keeps all "alive" track data in the radar sector (a track is erased if no update has taken place for 36 consecutive seconds).

d. Track Pool "POOL"

It holds tracks that have been successfully associated with report data, initialized tracks or reports which have been acquired during the last scan.

e. Shared Memory Update Buffer "Y"

It keeps the data that does not need further correlation, and is ready to update the subarea shared memory.

f. Exchange Buffers "Z"

They hold the track data of the regions where the radar sector overlaps with neighboring ones.

g. Exchange Buffers "RP OVER FLOW"

These buffers are filled only in cases where the number of reports loaded in "X" is greater than 40 (which is considered as the upper capacity limit for "X"). Its contents are the reports falling within the limits of the quadrant of the radar sector lying close to another radar sector. These reports are erased from the overloaded internal buffer "X".

h. Exchange Buffers "TR OVER FLOW"

These buffers are filled only in cases where the corresponding "RP_OVER_FLOW" buffers have been filled, and holds these tracks that lie within the same radar sector quadrants.

Note: Each radar sector is divided into the four principal quadrants (000-090, 090-180, etc.) In cases where an SBC which is dedicated to a particular radar becomes overloaded, its load is relaxed by a standby SBC which takes over the handling of target reports lying inside one or two quadrants until the original processor is no longer overloaded. When the situation at the "parent radar" sector is relaxed, the original processor takes over again the handling of the reports and tracks that physically belong to it.

The external view of a LCM is shown in Figure IV-3.

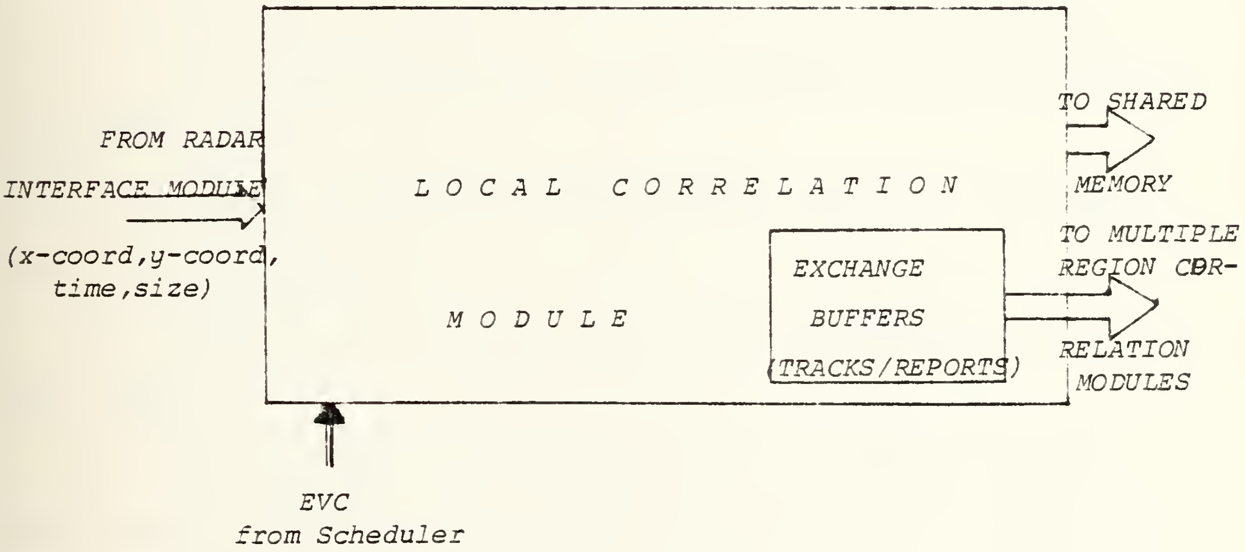


Figure IV-3. Local Correlation Module.

The internal view of the module (as described above) is shown in Figure IV-4.

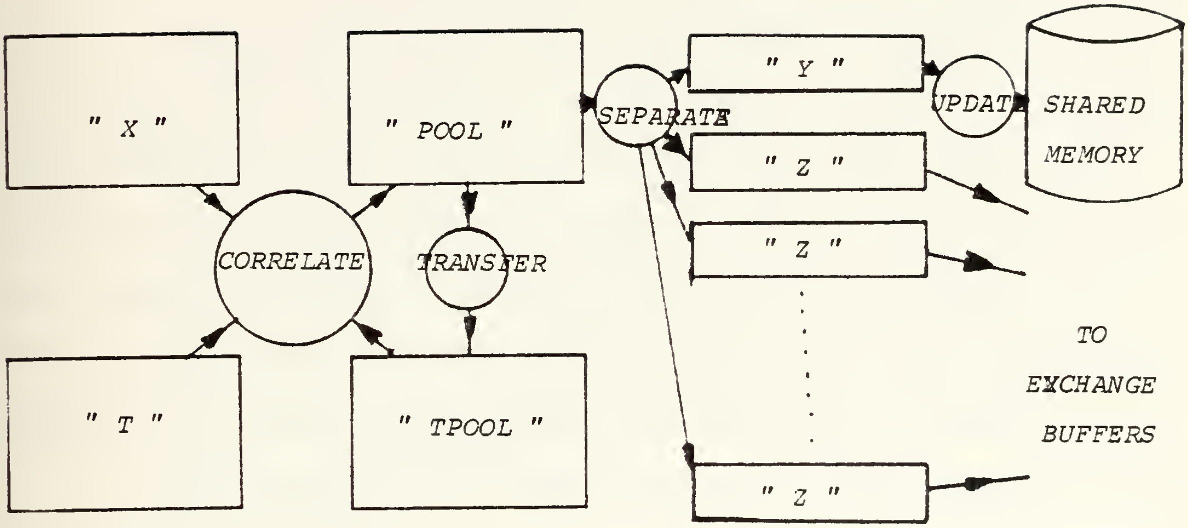


Figure IV-4. Local Correlation Module Internal View.

The operation of the LCM can be summarized as follows:

a. Track records are transferred from POOL to TPOOL, and POOL is cleared.

b. "Old" reports, and tracks are erased from both T, and TPOOL.

c. If the number of reports in X is greater than 40, then some of the data in the internal buffers X, T and TPOOL is transferred to standby processors (relaxed).

d. Reports in X are associated with "alive" tracks in TPOOL in two passes (one with the assumption that the target is moving with a constant velocity and heading, and the other

with a realistic change of these attributes). Each associated report/track pair is erased from X and TPOOL respectively, and is written into POOL.

e. Remaining reports in X are merged with reports in T, where track initialization is attempted. For each successful initialization, the track is written into POOL and these reports are erased from T. Reports which have not been used for track initiation are considered as initia reports and are loaded into POOL. At the end of this phase X must be empty. Reports and initialized tracks are assigned a track_no.

f. The reports in T which fall in a radar common region are loaded into POOL.

g. Tracks and Reports in POOL (which now all have their temporary track_number) are distributed according to their geographical position among the Y and Z buffers.

h. The shared memory is updated with track data in Y.

i. Buffers Z are unloaded into the EXCHANGE BUFFERS.

The following algorithms formalize the operation:

```
P1:                (corresponds to sector 1)
     do forever
          call await (evc(1), TH(1))
          input (radar buffer reports into X)
          empty radar buffer
          if no_reports  = 10 then
              if sum_reports  = 40 then
                  call de_relax(resume handling of passovers)
          call transfer     (track records from POOL to TPOOL)
          if no_reports    40 then
              call relax     (pass handling of some reports
                              and tracks to standby processor)
          call correlatel  (correlates/initializes tracks)
          call separatel  (separates tracks in POOL into Y,Z)
```

```
            output (tracks in Z to exchange buffers)
            empty buffers Z
            call update     (update shared memory from Y)
            call advance (evc(1,i)) (increment the event count
                                     of the common region cor-
                                     relation modules)
            TH(1) = TH(1) + 1
        end do
    end P1

    CORRELATE1:          (report-to-track correlation)
        clear TPOOL from "old" tracks
        clear T from "old" reports
        call pass 1    (extrapolate each track in TPOOL and
                        associate with each report in X by
                        report-to-track association)
        call pass2  (extrapolate each remaining track in TPOOL
                     associate and with each remaining report
                     in X by report-to-track association)
        call initialize  (merge reports in X and T into T,and
                          initialize new tracks by report-to-
                          report association).
    end CORRELATE1
```

"Await" and "advance" are synchronization primitives which are used to check if the event count has exceeded the threshold value (both passed as actual parameters), and to increment the event count respectively.

5. Common Region Correlation Module (CRCM)

The modules of this kind are of two types. The "dual-region", and the "triple region" ones. Their only difference is that the former handles the cases where target tracks exist inside the limits of two instead of three radar sectors overlapping regions. CRCMs are not executed by dedicated processors. Any one of a group of SBCs which is available executes them.

The input to these modules is a set of track records in the format described in the LCM subsection. Their output is updates to the shared memory.

The cycle is repeated every 6 seconds (one radar scan period), and can be summarized as follows:

a. Track-to-track association (two different radars).

b. Track number correction (when necessary).

c. Shared memory update.

d. For triple regions steps (1) and (2) are done twice.

The external view of these modules is shown in Figure IV-5.

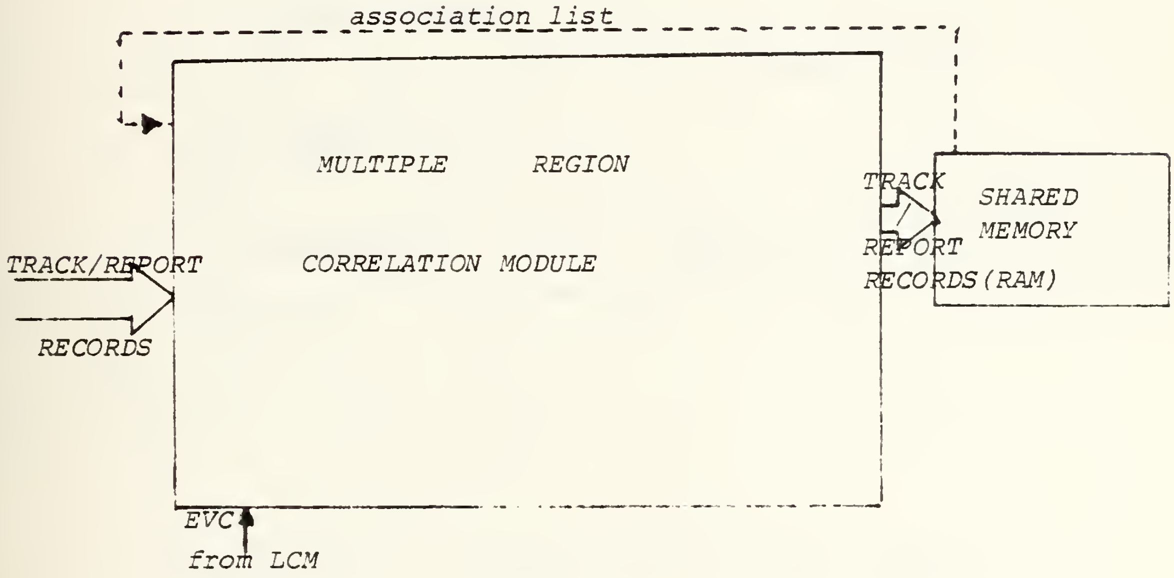


Figure IV-5. Common Region Correlation Module.

The following internal buffers are considered as necessary for its efficient functioning:

a. Buffers "Y1": They hold all track records as they are read from the various EXCHANGE BUFFERS.

b. Buffer "YR": It holds successfully associated tracks which are ready to update the memory module.

c. Buffer "YTR": It holds tracks successfully associated, and candidates for further association (only in triple common region correlation modules).

d. Buffer "AT": It holds pairs of track numbers which belong to tracks or reports that have been successfully associated in the past.

The internal views of a dual, and a triple CRCMs are shown in Figures IV-6, and IV-7 respectively.

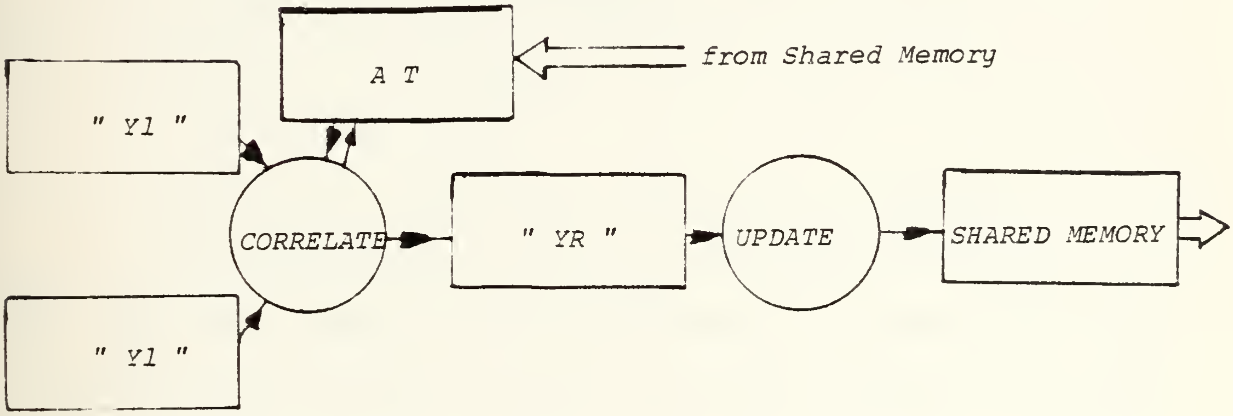


Figure IV-6. Internal View of Dual CRCM.

The operation of the CRCM can be summarized as follows:

a. Buffer AT (Associated Tracks) is loaded directly from the shared memory.

b. Each one of the tracks coming from the exchange buffer of one of the LCMs is associated with each one of the tracks coming from one of the exchange buffers of the other

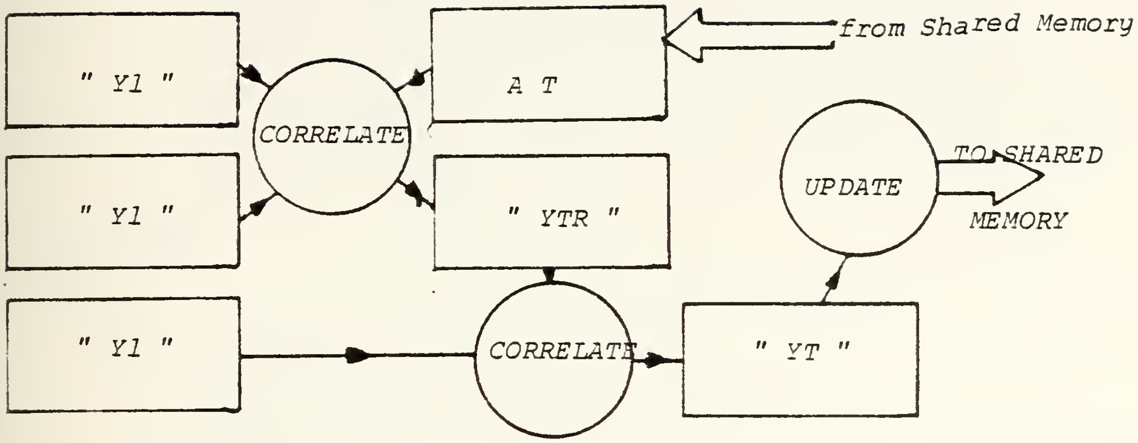


Figure IV-7. Internal View of Triple CRCM.

LCM. The track number of each successfully associated track is changed and the pair of these two track numbers is loaded into buffer AT.

c. Associated tracks are transferred to YR and erased from the Y1s.

d. Remaining tracks are transferred to YR (unassociated).

Note: For the triple CRCMs the remaining tracks are transferred to YTR, and the track-to-track association is repeated once more among the contents of YTR and the third Y1 (finally all reports are transferred to YR).

e. The shared memory is updated with the contents of YR, and all internal buffers are emptied.

The following algorithms describe the above functions in a formal way:

```
P12:             (common region of sectors 1 and 2)
    do forever
        call await (evc(1,2), TH(1,2))
        input (exchange buffers reports into Y1s)
        input (association pairs into AT buffer)
        empty exchange buffers
        call correlate2      (track-to-track associations)
        call update    (updates the shared memory from YR)
        empty buffers Y1, YR, AT
        TH(1,2) = TH(1,2) + 2
    end
end P12

P123:             (common region of sectors 1,2,and 3)
    do forever
        call await (evc(1,2,3), TH(1,2,3))
        input (exchange buffers into Y1s)
        input (association triples or pairs into AT buffer)
        empty exchange buffers
        call correlate2        (tracks of the two first Y1s)
        call correlate2        (tracks of remaining Y1, and
                                YTR)
        call update     (updates the shared memory)
        empty buffers Y1,YTR,YR
        TH(1,2,3) = TH(1,2,3) + 3
    end
end P123
```

Note: Indices in evcs and THs refer to the serial numbers of the radars involved in the cross-correlation.

6. Scheduler Module (SM)

This module controls the whole operation of the radar complex of the surveillance system. Its only output is the so called "sixsec_evc" which flags the start of each new scan period (6 seconds) and comes from a local clock. This is synchronized by the multiprocessor control module complex through a synchronization message. Its outputs are two kinds

of event counts, interface modules, and one to the local correlation modules (rad_evc and evc respectively).

The SM is executed by a dedicated SBC. This module also controls the operation of the clock and initiates the unloading of all track report data residing in the shared memory into the local memory module and the multisensor correlation complexes which further associate them with data gathered by other sensor systems.

Its functionality can be better shown in the following algorithm:

```
P:
    call start      (start the system and the global clock)
    do forever
        call await(six_evc, TH)
        for each evc set do
            call advance(rad_evc(i))    (for the ith radar
                                         interface module)
            call advance(evc(i))        (for the ith cor-
                                         relation module)
            call mem_unload ()
        end do
        TH = TH + 1
    end do
end P
```

7. Shared Memory

The shared memory of the radar module complex is a 64K RAM memory which holds both data and processes. The data stored there are the track records, the unassociated reports and the track_number association pairs/triples mentioned in the previous paragraphs. All these refer to the currently tracked platforms. All the processes used in the module complex are stored in the shared memory. The space blocks occupied by processes and data are predefined.

Whenever one of the CRCMs is invoked, a nondedicated processor (SBC) of the complex is utilized, the proper process is loaded into the SBC's own memory and execution begins.

The block of the shared memory holding the track/report data is transmitted on the bus to the multisensor system correlation, local memory and I/O module complexes of the multiprocessor node. This action is controlled by the SM. Figure IV-8 shows how the shared memory of the radar module complex is divided.

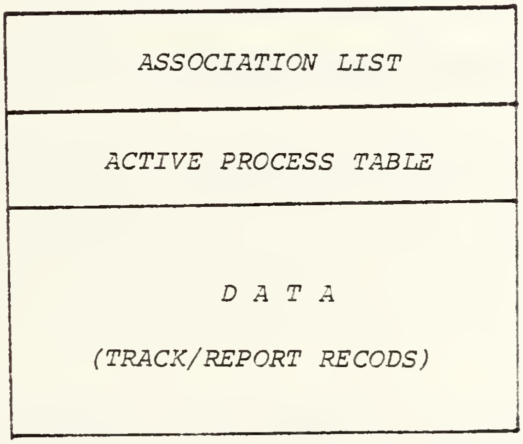


Figure IV-8. Shared Memory Division.

8. Module Integration

Since all module's internal structure has been described in detail, the integrated system consisting of all the above is shown in Figure IV-9. All links between the processes are marked.

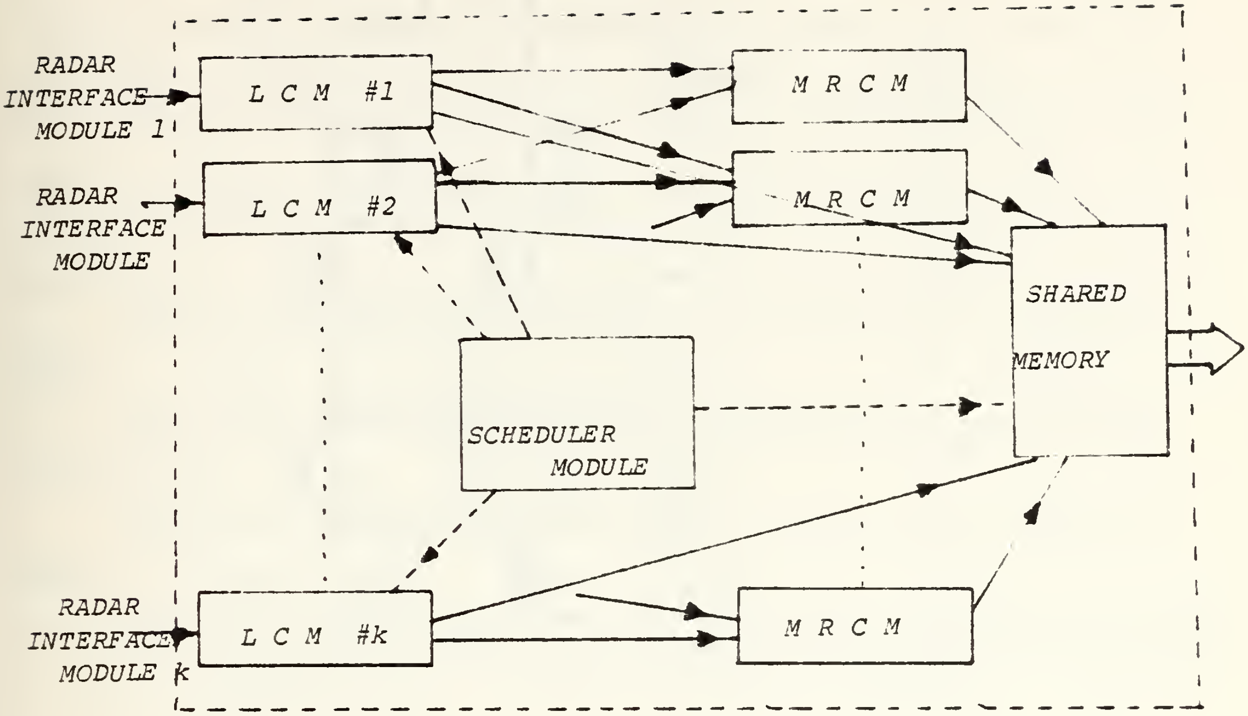


Figure IV-9. Integrated System's View.

The time that is required by the radar module complex to perform the correlation of all data collected over one radar scan period is critical to the operation of the whole system.

A time analysis of events is shown in Figure IV-10. There, the required time each one of the processes takes to process a maximum number of 40 "active" tracks is given in scale. These maximum times (6 seconds) correspond to the time it will take to perform 40 track initializations (40 reports on the last scan and about a hundred of previous scan reports in buffer "T" taken in triples in all combinations). Also the actual time a given sample of report data

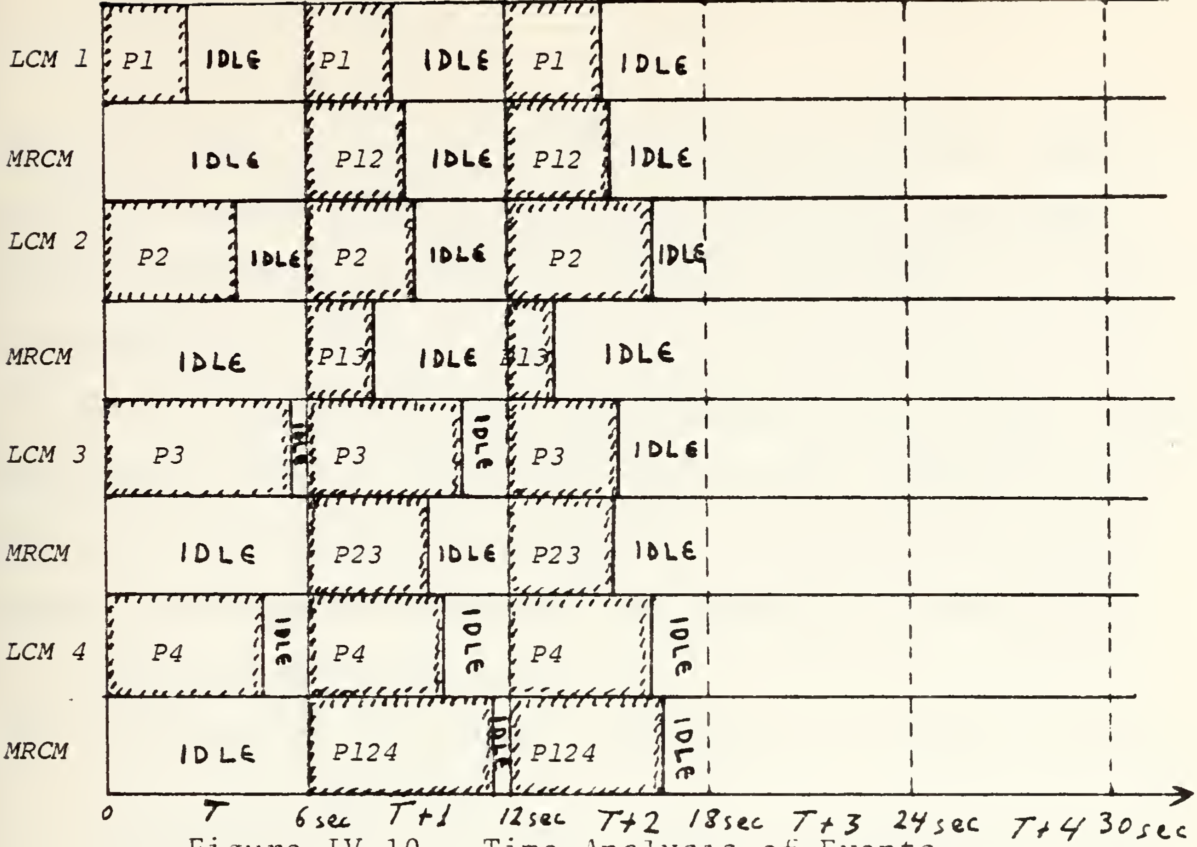


Figure IV-10. Time Analysis of Events.

takes to be manipulated is indicated with shadowed boxes within the 6 sec boxes. If the process terminates sooner than in 6 seconds, the processor stays idle until the data of the next scan period arrives.

B. DATA CORRELATION

One of the critical functions of the radar module complex in the multiprocessor node is the synthesis of radar information about enemy, friendly, and unknow identity ships, submarines, aircraft, and missiles in the subarea.

In order to cope with the situation, modern ocean surveillance systems had to become computerized. What computers are called to do is to replace human operators in target tracking and classification (partially). Both of these

processes rely primarily on the correlation of data items referring to the various targets in the area. This data either preexists in a data base, or is collected by a chain of sensors.

The required output of a computerized surveillance system consists of a set of resolved target tracks, followed by as much extra information as desirable. In order to do these tasks, the following steps must be completed in real-time:

a. Track update/initiation.

b. Calculation of more geolocation data (velocity, heading, etc.) for each track.

c. Estimation of additional constant, and discrete track characteristics.

The above steps directly imply the use of data correlation (or association) algorithms. A great variety of such algorithms have been developed over the last 20 years. Some survey papers [Refs. 12, 22 and 23] reflect most of these efforts. In addition, a project by the Naval Research Laboratory (Washington, D.C.) has produced a great variety of papers and reports on the subject. The Naval Ocean-Surveillance Correlation Handbook project [Refs. 6, 24] is an overview of the existing literature in this area. It also summarizes the major topics of research towards more efficient correlation algorithms (in terms of speed and reliability).

Most of the existing algorithms provide for multiple target tracking, track initiation, isolation of false alarms, coping with missing measurements, and other general or special

cases (as merging, splitting, etc. of tracks) which will be analyzed in more detail in the following sections. Among them, there is a group of algorithms which imply "multiple-scan correlation", "sophisticated data partitioning", "recursiveness", and take advantage of the discrete in addition to the continuous target characteristics. These algorithms are faster than the rest.

The present section overviews the general surveillance correlation algorithm characteristics. It further concentrates on the ones used by this system.

Correlation algorithms can be categorized into report-to-report, report-to-track and track-to-track. Each one of them is utilized during a different phase of the correlation process.

1. Clarifications

Some clarification is considered necessary for understanding correlation algorithms in general as well as for the specific ones used by the proposed system. Collected data must be associated with data existing in some storage area. This way, the most reliable information can be derived for each individual target within the limits of the surveillance area, and the decision-makers will have a clear picture on which to base their decisions.

The region is scanned in three dimensions (air, surface, and subsurface), with the objective of collecting as much reliable information as necessary, primarily on

hostile or potentially hostile targets (geolocation, discrete, and constant characteristics).

REPORT: A formated description of an observation by a sensor of the surveillance system. Each report includes a time of observation plus geolocation data (range and bearing from the radar position).

SCAN DATA: A set of reports coming from the same radar, which were obtained during a scan period. At most one report of a scan refers to each target in the area.

TRACK: A set of reports obtained over an extended time span, which are judged as relating to the same platform.

FALSE ALARM: A contact detection coming from a sensor, not originating from a real target.

TARGET CORRELATION: The decision that two or more elements in the set of collected data have a specific relation.

2. Overall Correlation

When the sensors of the surveillance system are locally separated (as for the system described in this thesis), the conversion of the incoming geolocation data to a common coordinate system is unavoidable. The general approach to the multiple site correlation problem is to sequence through the tracks of a given site and examine each one of another site's tracks in order to determine which track, if any, originates from the same object.

Morefield's methodology [Ref. 25] is considered as very representative of the case. The method is illustrated in Figure IV-11 below.

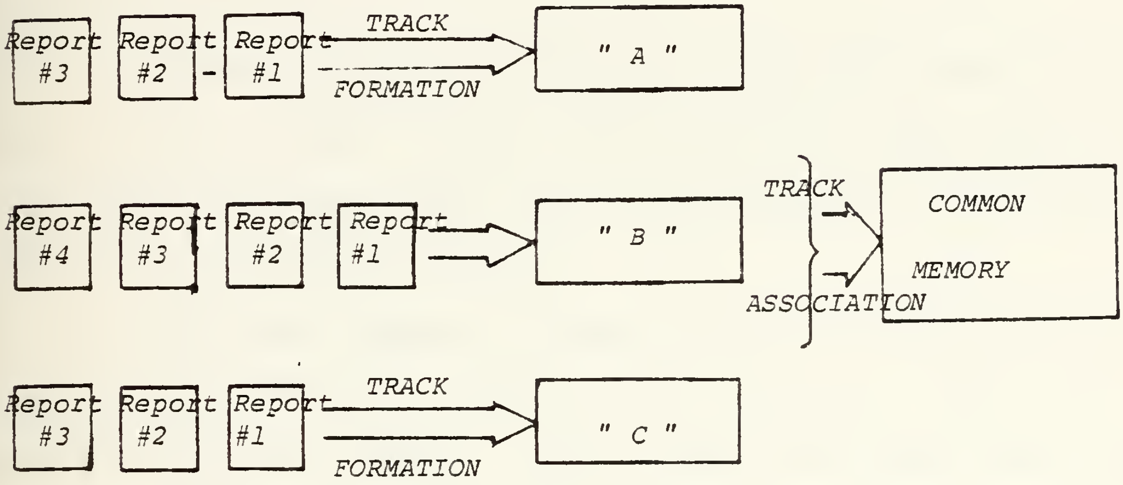


Figure IV-11. Morefield's Method.

According to this method, reports collected by each individual sensor are correlated separately at the local (radar) level. This correlation has two main tasks; (a) to update existing tracks (report-to-track association), and (b) to associate individual reports in order to initialize tracks or isolate false alarms (report-to-report). A local data set is formed, which includes all resolved track coming from the individual radar reports. On a second phase, a track-to-track correlation algorithm is implemented to integrate tracks of the local data sets into a global data base.

This way, tracks of the same object held by more than one radar are identified and a clear picture is offered to the decision-maker. The same approach is taken by Bowman [Ref. 26] (he uses a maximum likelihood approach). In this later work, the issue is extended to include different generic types of sensors.

During the first correlation phase the polar coordinate system is used. Before entering the second phase (track-to-track) positional data has to be converted to the global cartesian coordinate system.

The usual approach taken in most of the correlation algorithms is carried out in terms of "passes" based on a "most likelihood" scheme. Reports are associated with existing tracks according to the criteria of how well they fit on a straight line (heading) and on regular intervals (constant velocity). Tracks of this family are called "well behaving". Subsequent passes are treating the so called "less well behaving" tracks in an increasing difficult sequence. Reports which are correlated are removed from further consideration. The remaining data is analyzed according to different criteria, etc. This stepwise correlation methodology is discussed in more detail by Wiener [Ref. 27]. Figures IV-12, IV-13 and IV-14 illustrate the stepwise correlation. This method is utilized for the conceptual surveillance system of this thesis because of its simplicity.

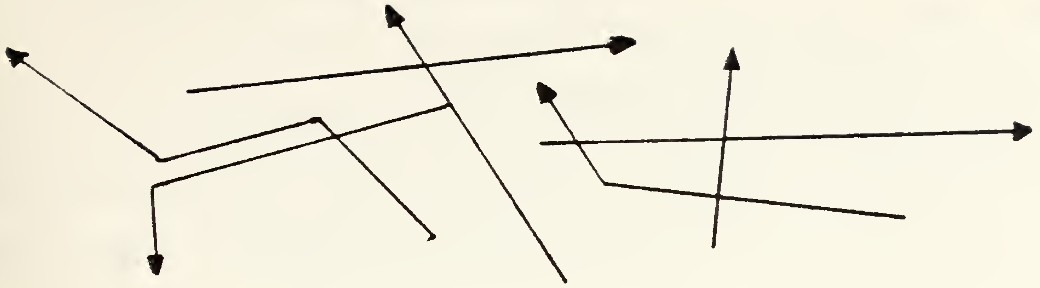


Figure IV-12. Initial Picture.

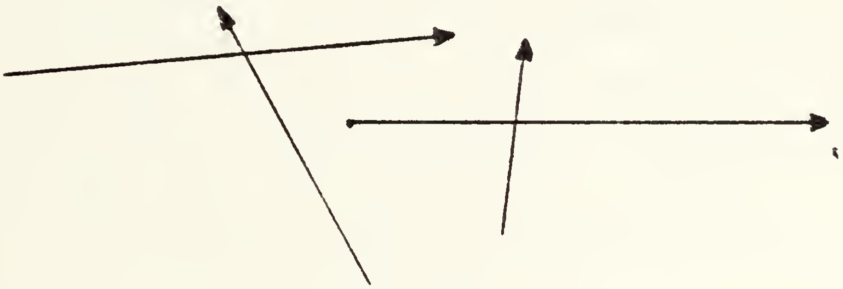


Figure IV-13. Well-Behaving Tracks.

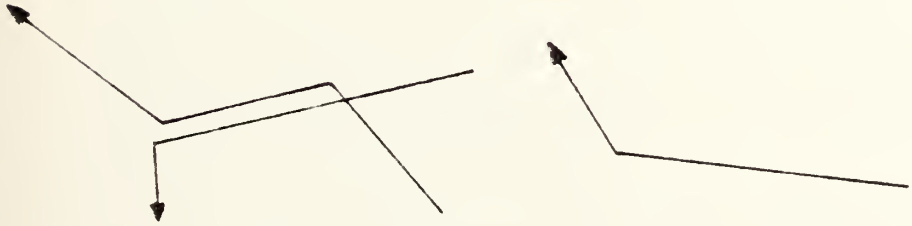


Figure IV-14. Second (final) Pass.

3. Report-to-Report Correlation

Correlation is performed by associating data reported over a scan period with data reported during the same scan period by another radar, or data reported by the same or other radar on the previous scan period. It is used in two cases.

The first is when there are two radars with overlapping detection sectors and it is desired to determine for each specific individual report if it comes from different targets (each one detected by one of the radars). An assumption which has to be made in order to implement this kind of correlation algorithm is that the reports refer to the same or almost the same time. The mathematical formulation of the problem is expressed by the following equations:

$$z(1) = x(1) + v(1) \text{ [radar \#1]}$$

$$z(2) = x(2) + v(2) \text{ [radar \#2]}$$

where $z(i)$ represents the position as reported by radar i,

$x(i)$ is the actual target position,

and $v(i)$ is the position report error of radar i.

If the reported positions $z(i)$ belong to the same target, their Pythagorean distance has to be less than, or equal to the two radar's measurement error. Otherwise the reports refer to different targets.

The second case, where report-to-report correlation is used, appears while trying to find candidates for track

initiation at the single radar level [Ref. 24]. The case is briefly addressed here. In case there exists information on the maximum, and minimum velocities of the observed target, an annulus can be drawn which is centered on one of the two subsequently reported positions. The inner diameter of the annulus will be the minimum, and the outer diameter the maximum target velocity. These are multiplied by the elapsed time between the two reports. Positional data are positively associated if one of the positions falls inside the other's annulus. When only a maximum velocity is known the annulus becomes a circle. Finally, when neither the minimum nor the maximum velocities are known, an "absolute maximum velocity" replaces the second (Figure IV-15).

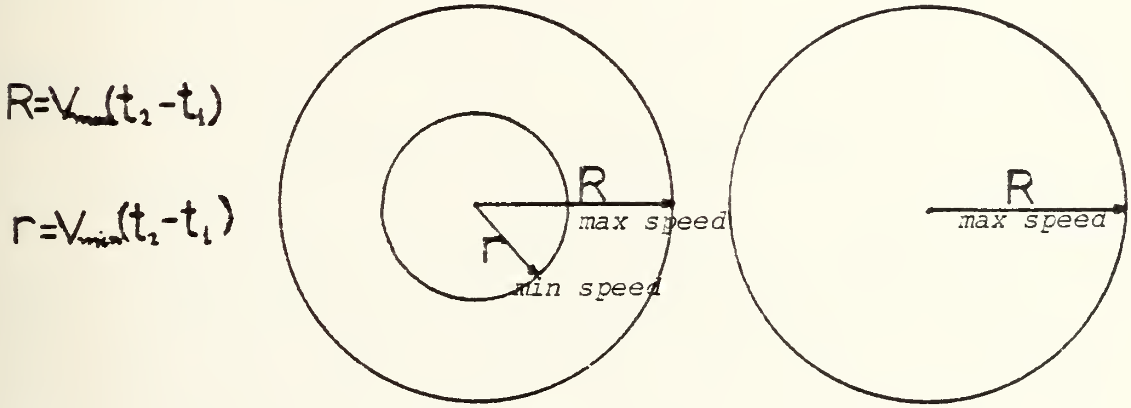


Figure IV-15. Heading Unknown.

In cases where the reports include heading information as well the annulus becomes an annulus sector and the circle becomes a circular sector respectively (Figure IV-16).

When the reports include extra discrete data, special cases apply [Ref. 24].

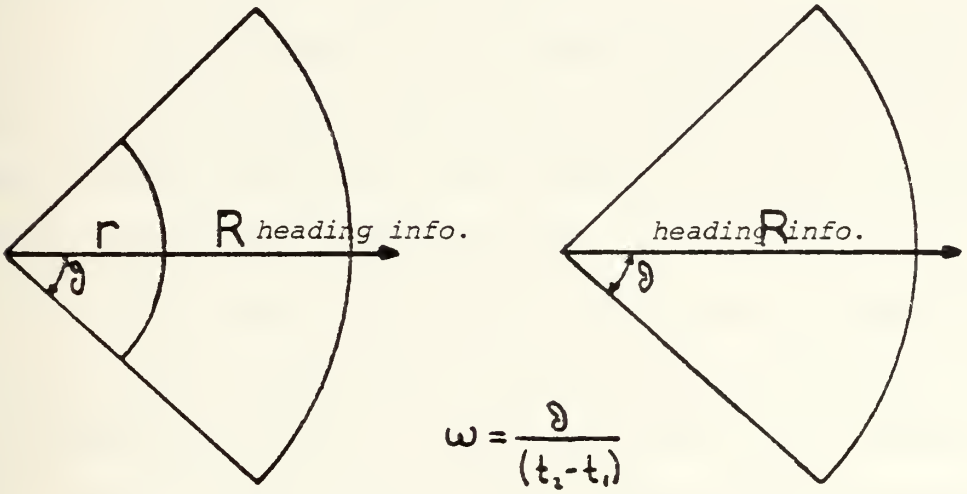


Figure IV-16. Heading Known.

It is clear that track initiation ambiguities need not be resolved based on only two consecutive reports. If required, more reports should be considered. It must be kept in mind that as the number of unresolved tracks and the number of scans grows, the number of hypotheses to be considered increases exponentially and the system quickly becomes overloaded.

4. Report-to-Track Correlation

This category of correlation processes is based on the assumption that a file consisting of track records already exists. Scan data coming from a sensor system is associated with these existing tracks. This method is more suitable for data partitioning. Each track consists of geolocation, discrete, and fixed attributes.

The geolocation information has to include: (a) positional history of the track, either over a fixed time-span or expressed as a fixed number of consecutive position reports, and (b) heading/velocity information.

The number of past positions kept in each track record varies from application to application. Whenever a new set of reports is injected into the system, the probability density for the position of each track is dead-reckoned to the time of this report. This way, measures of report-to-track correlation are developed (e.g. distance between the projected track, and the observed report). The resulting measures of correlation plus data on present reports are used to update the tracks into the track file. If in the definition of "data" one-point-tracks are accepted, then report-to-report correlation can be viewed as a special case of report-to-track.

Most of the special cases can be handled more efficiently by using report-to-track correlation algorithms. Some of these are track splitting, merging, deletion, missing reports, and false alarm handling. Dense target, land proximity,

and clutter environment situations are also better handled in the report-to-track approach.

5. Track-to-Track Correlation

This case can be considered as including the report-to-report and the report-to-track (a report is a special case of a track) correlation. The situations where its use is needed are:

a. When there are two cooperating (neighboring tracking) systems, each maintaining its own track file. In this case the procedure followed can be analyzed into (1) the correlation of tracks coming from both of these systems, (2) the determination of the ones which are duplicates, and (3) the creation of a global data base where each track is referenced once.

b. When dealing with different generic classes of sensors (e.g. radars, active sonars, ESM, hydrophones, IR detectors, etc.) In this case it is preferred to integrate these classes of information, and create a more complete track description scheme.

Since information on each one of the track files is referred to different times a series of interpolations must be performed for the data of both tracking systems. These interpolations are followed by a series of point-to-point associations. It is obvious that this category of algorithms is more time consuming, but it is unique for the case of neighboring surveillance systems. This method is used in

the Common Region Correlation modules of the radar module complex in the multiprocessor nodes of the system.

C. TRACK IDENTIFICATION

As described in the previous chapter and in Appendix A, a track record has a number of elements which are considered as necessary for its association and/or display. A more detailed description of the elements of the track record is provided below.

1. Track Record Format

The format of the track records as they are produced by the Local Correlation module is as follows:

TRACK

(time1, time2, time3, x_coord1, Y_coord1, x_coord2, y_coord2, x_coord3, y_coord3, heading, speed, size, track_no, id, type)

time1 corresponds to position 1 (it is expressed in hrs, min, sec)

x coord, y coord are fractional numbers expressing the x, y coordinates of the position in Km

heading is expressed in whole degrees,

speed is expressed in whole knots.

track-number is an integer with the first two digits denoting the identity of the detecting radar (e.g. 01,02,...), and the remaining ones its sequence number referring to the radar (when 60 is reached we start assigning the emptied numbers from 0 and on).

id is a three-digit integer whose last digit represents one of the following:

0: friendly

1: enemy

2: neutral

3: unknown

type is a three-digit integer whose first two digits correspond to the type of the target as follows:

00: military aircraft
01: warship
02: military helicopter
03: submarine
04: missile
05: unassigned
06: merchant aircraft
07: merchant helicopter
08: merchant ship
09-11: unassigned

The last digit defines the specific type of the vessel (e.g. 011 is aircraft carrier, etc.)

Note: Mechanisms for the determination of the three last track attributes have not yet been incorporated.

2. Track Number Allocation

Each track or unresolved report coming from a given radar is assigned a track_number. This track number is formed as described in the previous paragraphs. The allocation of the track numbers is done by each Local Correlation module. This module accounts for the assigned and unassigned track numbers.

Track numbers assigned to tracks or reports lying outside the common regions of overlapping radars keep their assigned track numbers. For the ones that are detected inside the common regions, permanent track numbers are assigned by the common region correlation modules.

When a report, detected by two different radars, comes to this module, it is assigned the track number given by the local correlation module serving the radar that detected it first.

Subsequently, both of these track numbers are stored into a so called Association Track buffer (AT) in the multiple common region correlation module. This way, whenever one of the Local Correlation modules sends the same record (track or report) to this module, tedious correlations are avoided. The track number passed to the shared memory of the radar module complex is the one assigned by the initial detector.

D. TACTICAL SITUATION ASSESSMENT

As was previously mentioned, target classification is very important in surveillance systems. Morefield, Bowman and Murphy address the subject of tracking and recognition concurrently [Refs. 28, 29]. Their correlation scheme considers all sensor reports together to form the "best estimate" of the "surveillance volume". The general algorithm can be described as follows (see also Figure IV-17):

1. Express the reports (from a variety of sensors) in common terms.
2. Generate feasible correlation hypotheses.
3. Evaluate feasible correlation hypotheses.

The approaches of Smith/Winter [Ref. 30], Smith [Ref. 31], and Witte/Lucas [Ref. 32] treat the subject from the pattern recognition aspect. The latest approach (1) avoids maximum likelihood decision techniques, (2) automatically identifies areas of data inadequacy, and (3) permits the realization of the full implication of ambiguous data.

Fortman, and Baron address the tracking problems encountered in using sonars [Ref. 33]. They discuss the limitations of underwater surveillance imposed by both active and passive sonars, by the environment and by the targets themselves. Their correlation algorithm is a suboptimal one (they are using an Extended Kalman Filter). Even if geolocation data does not have high accuracy, doppler radar data has a unique characteristic which indicates movement and gives a positive classification clue. A more recent paper by Fortman, Bar Shalom, and Scheffe [Ref. 34] introduces the Probabilistic Data Association approach into sonar applications. Their algorithm is also limited to passive sonars only.

Algorithms that more effectively handle the multi-target/multi-sensor case in cluttered environments have been created by Reid and Goodman [Refs. 23, 35].

A radically different approach is the one taken by Friedlander, and Anton [Ref. 36]. Instead of treating the basic detection and location estimation separately for each target, a simultaneous estimation of multitarget locations is made. The two key ideas used are: (1) the formulation of the multitarget problem as a multichannel estimation one, and (2) the representation of the multisensor data by the parameters of a model which fits all the available data. Friedlander has expanded this work some more [Ref. 37].

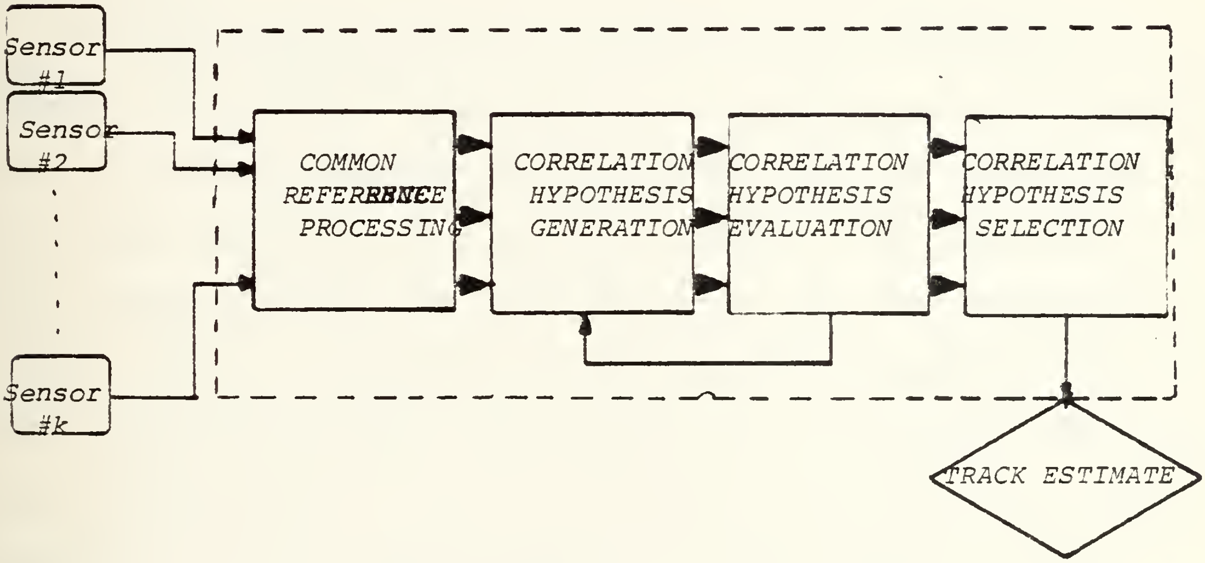

Sensor #1
Sensor #2
Sensor #k
COMMON REFERENCE PROCESSING
CORRELATION HYPOTHESIS GENERATION
CORRELATION HYPOTHESIS EVALUATION
CORRELATION HYPOTHESIS SELECTION
TRACK ESTIMATE

Figure IV-17. Flowchart for Multi-target Multisensor Correlation.

Papers which are more oriented to the ocean surveillance target tracking are [Ref. 12] by Reid and [Ref. 38] by Atkinson. The last deals with the problem of developing a quantitative and physically meaningful measure of association,

by comparing the discrete attributes contained in the report of a tracked target with the continuous ones. The final association derives additional information by comparing position/velocity and discrete characteristics or emissions.

E. THE HUMAN INTERFACE

The last and one of the most crucial functions of any surveillance system is the alertment of the decision-maker(s) in order to initiate responses to developing threats. This can be accomplished through a variety of man-machine interface means.

The way information is presented in this conceptual model of the surveillance system is by means of video displays on large screens and private (one man) consoles. Two kinds of visual information is provided, graphic and alphanumeric. The graphic information is categorized into land masses and active tracks. Alphanumeric information is supplementary to the graphical and gives descriptional information. There exists an option to display the active tracks only (not land masses). This is chosen manually by the operator of each individual display.

Land mass information is stored into a separate memory attached to the display system complex. Each one of the memory clusters is a block corresponding to a 10 X 10 sq. miles area on the global tactical grid. Land information occupies the first of the records in each block and track

information follows. Since land occupied area does not change, the address where the first track record is stored is fixed in each one of the blocks. This way the "no land" option of display can be chosen at any time.

The operator can select the dimensions of the area he wants to have displayed. The minimum area that can be displayed is 10 X 10 sq. miles (the area covered by one memory block). Next, he can increase the area by incrementing the number of blocks by the square of the next one block increment (e.g. 10 X 10, 20 X 20, 30 X 30, ..., n*810 X n*10).

In Figure IV-18 the architecture of the Human Interface Module (HIM) complex is shown.

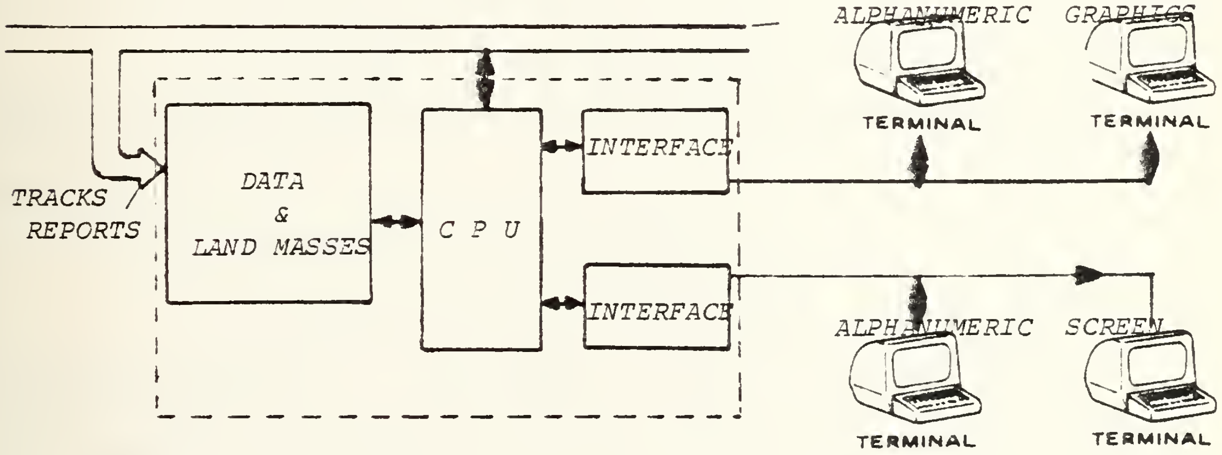


Figure IV-18. Human Interface Module Complex.

The operation of the HIM is controlled by the Scheduler of the multiprocessor node. Each time new target data is transmitted through the bus (every scan period) it also goes to the HIM. There the data is loaded into the display memory. Just after data transfer is over the interface module takes over and displays the data on the video consoles or screens.

Whenever the operator wishes to interact with the system in order to switch to the "no-land" display mode or to request additional information on a specific target, this interaction also goes through the interface module.

For the console display the hardware/software arrangement is similar to the one described by T. Boone in Reference 46.

1. Hardware

The hardware necessary for the implementation of the display is listed below:

a. SBC 310 Mathematical Processor

It is used to manipulate the data of the display memory in order to convert it into a convenient form for display.

b. AN/UYQ-10 Plasma Display Set

It consists of two alphanumeric and graphics display terminals. The graphics display terminal allows the operator to interact with the display system by touching a point on its front screen surface. By touching the position where a target is projected on the plasma display screen infrared lightbeams which form a rectangular matrix near

the surface of the screen are interrupted. The position of the finger on the screen can be determined and hence a simple human interface can be set up.

c. RG-512 Board Equipped Terminal

This system as both alphanumeric and graphic capability. The terminal has a feature which permits selective erasure of vectors, points or characters.

2. Process Organization

There is a family of processes which controls the operation of the Human Interface Module. These processes are listed in detail in Reference 46 and they generally perform the following functions:

a. Display targets on the AN/UYq-10 Plasma Display Panel. Different symbols indicate the type (surface, air, subsurface) and the classification (friendly, hostile, unknown) of the targets.

b. Permit the user to interact with the system and change the display menu.

All the software for the implementation of the above HIM complex in PLI is included in Ref. 39.

F. COMPONENT FAILURE DIAGNOSIS AND SYSTEM REORGANIZATION

The multiprocessor node has several internal mechanisms for the diagnosis of component failures. These mechanisms initiate procedures to reorganize the system. Finally, when one of the failed components becomes operational again, some recovery steps are taken. A description of some of these fault tolerance mechanisms follows.

1. Node Bus Failure

In case the common bus of a multiprocessor node fails, the secondary bus takes over. The failure is sensed by the Scheduler module of the module complexes which is receiving a synchronization signal from the control complex every 1/10th of a second (event count). Immediately after detecting the failure, all Scheduler Modules force the switch to the bus to flip to the secondary bus and data flow continues as before.

On the average the data lost is limited to the data flowing on the bus on a 0.05 second time span. Depending on what that information is, the loss may be serious or not. The most serious loss of data occurs whenever data heading for the channel interface unit is lost. On the other hand, this is the most improbable case since the probability of such a loss is 0.00055 (the information will be delayed by 3 minutes if it is for an update, or 6 seconds for initial report).

The flipping of the bus switches of the module complexes activates an audio announcing mechanism which alerts the operator(s) to take corrective action and restore the failed bus. After restoration the faulty bus, it will act as a secondary one.

2. Sensor Failure

The failure of one of the sensors is, in most of the cases, causing a gap in the surveillance net (unless the

system provides for coverage of any point in the surveillance area by multiple sensors).

The failure is sensed by the Radar Interface Module (RIM) which sends a special message to the Scheduler through the dedicated SBC of the Local Correlation Module. The Scheduler, receiving such a failure announcement, suspends the use of all Dual Region Correlation Modules (CRCM) where data sensed by the failed sensor was being correlated with others. Instead, the data coming from the other LCM of the pair goes directly to the shared memory of the complex.

While the sensor is down, its dedicated SBC stays idle. After sensor recovery, the SBC starts its operation again attempting to initialize tracks since all the "old" data has been lost.

3. SBC Failures

a. Dedicated SBCs

Their failure is sensed by the Scheduler through the event count mechanism and their task is switched to the standby SBCs. The latter have to assume that no track information exists, so they start initializing tracks from the beginning.

b. Nondedicated SBCs

Their failure does not cause any problem to the operation of the node since any one of them can perform the job. Only the data correlated during the present scan period is lost. The only case in which such a failure may cause

more serious problems is when a great proportion of the non-dedicated SBCs fails and the remaining ones are not able to take the processing load. The last case seems most unrealistic and it implies that many other failures have also occurred to the system.

4. Shared/Common Memory Failure

Two copies of the shared memory is kept on each module complex. So, whenever a mechanical failure is detected in one copy, the other copy is used instead. The same arrangement is provided for the Local Memory Complex (two RAM units are used).

G. OVERLOADS AND SYSTEM'S RESPONSE

Under the architecture of both the multiprocessor node and the individual module complexes the cases where overloads can occur are limited.

Data which has not been filtered is not allowed to flow on the bus of the multiprocessor node. This reduces the bus's load. Only prefiltered data and control messages flow. These are unable to saturate it. The same can be said for the buses of the individual module complexes.

Overloads can occur only at the Local Correlation Module's level whenever the capacity of the dedicated SBCs is exceeded. This can happen in cases where the number of the reports arriving from the Radar Interface Module is greater than 40. This means that in a certain radar's sector the density of

targets has exceeded the preestablished 0.07 targets/sq.Km. In such a case, the data associations which are to be performed for both report-to-report and report-to-track correlations demand more than 6 seconds processing time.

To cope with this overload case, a special relaxing mechanism is provided, which is called to execute a process similar to the one executed by the overloaded SBC. This "relax" technique is described as follows:

1. Each circular radar sector is subdivided into four equal sectors (the 4 principal quadrants) starting from bearing 000.

2. A mechanism is introduced, which counts the incoming reports into the internal buffer "X". The mechanism counts the total number of reports plus the number of reports on each one of the 4 quadrants.

3. If the number of reports in "X" exceeds 40, then, starting from quadrant "A" (000-090), the number of reports in "A" is subtracted from the total number of reports in "X". If the result is a number (of reports) less than or equal to 40, the reports lying within the limits of "A" are transferred to a standby process served by an extra processor.

4. If the subtraction of the reports in "A" is not enough for the overloaded sector processor to be relaxed, the reports quadrant "B" (next quadrant clockwise) are subtracted (only two quadrants can be serviced by the standby process).

Note: Subtraction always starts from the quadrant which has the greatest number of reports.

5. At the same time, the records of the tracks, as well as the unresolved reports (internal buffer "T") lying in these pass-over quadrants, are also transferred to the standby process.

6. When the number of reports in "X" drops below 10, then, if the sum of reports in the internal buffers "X" of both the original sector process and the standby one, is less than 40, the original process takes over again.

The above mechanism allows the Local Correlation Modules to be executed within the 6 second time frame. Figure IV-19 illustrates the mechanism.

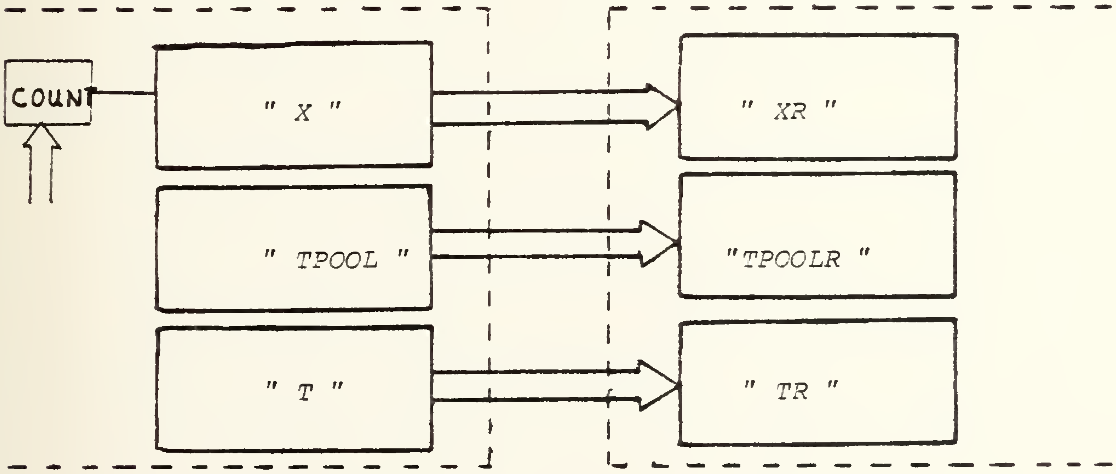


Figure IV-19. Relaxing Process Mechanism.

The described mechanism has the ability to increase the sustainable target density up to 0.14 targets/sq.Km. No other notable overload cases are believed to be possible at the multiprocessor node's level under the present system's design.

V. PERFORMANCE PREDICTION AND EVALUATION

A. LINEAR PERFORMANCE IMPROVEMENTS WITHIN THE NODE

The architecture used in the individual nodes of the proposed surveillance system offers a variety of advantages in terms of response time and throughput. Most of the advantages are a result of the proposed implementation of the multicomputer system described in the previous chapters. On the other hand, the system is untried and requires a complex operating system to control its operation.

The introduction of multilevel busing (two levels) makes the system similar to the C.mmp and C.m* [Ref. 40]. In these systems the concept of multiple level of busing was first introduced and offered a substantial decrease of the load on these buses whenever the application allows concurrent (and especially filtering) computations. This way, contention for the use of the bus is reduced and bottlenecks become more improbable.

An analysis of the improvements in both the throughput and the response time for this category of multicomputer systems is provided in Ref. 41. In order to implement this analysis technique to the proposed multicomputer schema at the node level, it is assumed that 4 radars are contained in the radar group controlled by the Radar module complex of the multiprocessor node. These radars are numbered 1 to 4

and the pairs 1-2, 2-3 and 1-4 have overlapping sectors. In addition, radars 1, 2 and 3 have a triple common region of sector overlapping.

Assuming that the complexity of computations is such that:

-Each Local Correlation Module (LCM) takes 3 seconds to execute,

-each Dual Common Region Correlation Module (CRCM) takes 3 seconds

-and the Triple CRCM takes 2.5 seconds.

If one SBC was available, then the total execution time between the unloading of the SCAN REPORT BUFFERS and the completion of the correlation process would be 20.5 seconds (sum of the above times). This time should then be doubled if a cross-correlation is required between data produced by the radar group and another sensor type group (e.g. sonar).

By using the multicomputing scheme proposed in this thesis, this time can be reduced to 5.5 seconds (for the Radar module complex level). This reduction requires the use of four SBCs. The time lines of module execution for one and four SBCs respectively are shown in Figures V-1 and V-2 (P1, 2, 3, 4, 12, 14, 23, and 123 are correlation processes corresponding to radar sectors and common regions).

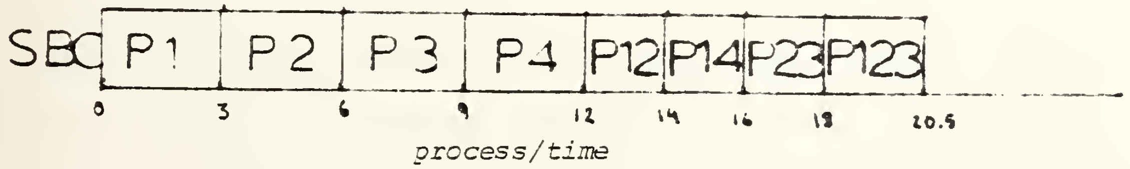


Figure V-1. Time-Line Analysis with One SBC.

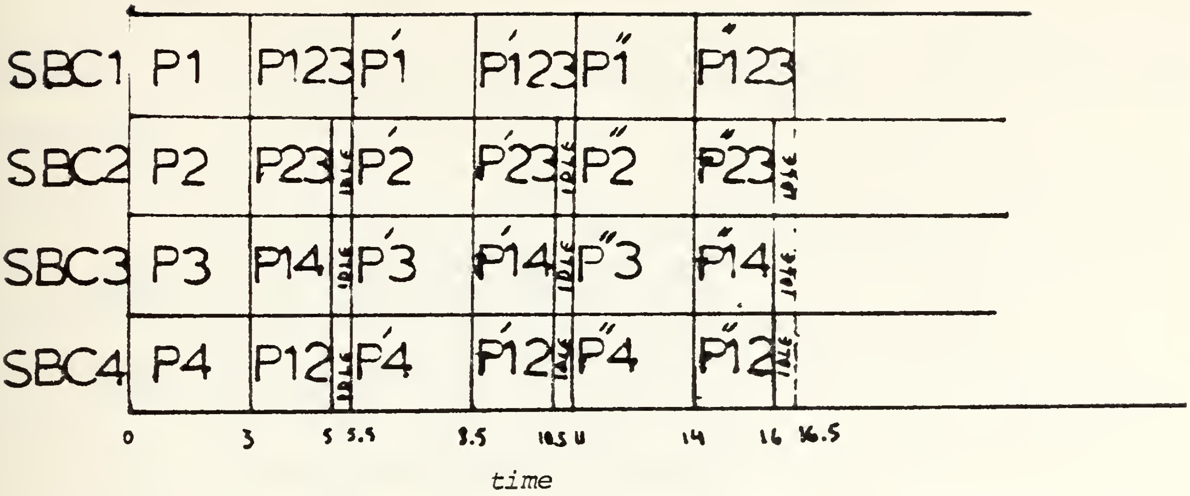


Figure V-2. Time-Line Analysis with Four SBCs.

Note: For the proposed system, the execution of the processes P1, P2, ...does not take a fixed amount of time. Irrespective of this, the time-line analysis of the execution of the processes by the multicomputer system looks similar.

The above figures illustrate the minimization of the system's response time. To maximize the throughput, four more SBCs have to be utilized in such a way that while the four first ones are busy executing the LCMs, the remaining are used for running the CRCMs for the data of the previous correlation cycle of the system (radar scan periods). This is illustrated in Figure V-3.

The above improvements can at the best increase the processing power of the system linearly [Ref. 41]. By adding more SBCs to the system (more than 8) no further improvement

is achieved with the proposed set of processes (however more computers can be useful for backup purposes in case of a SBC failure).

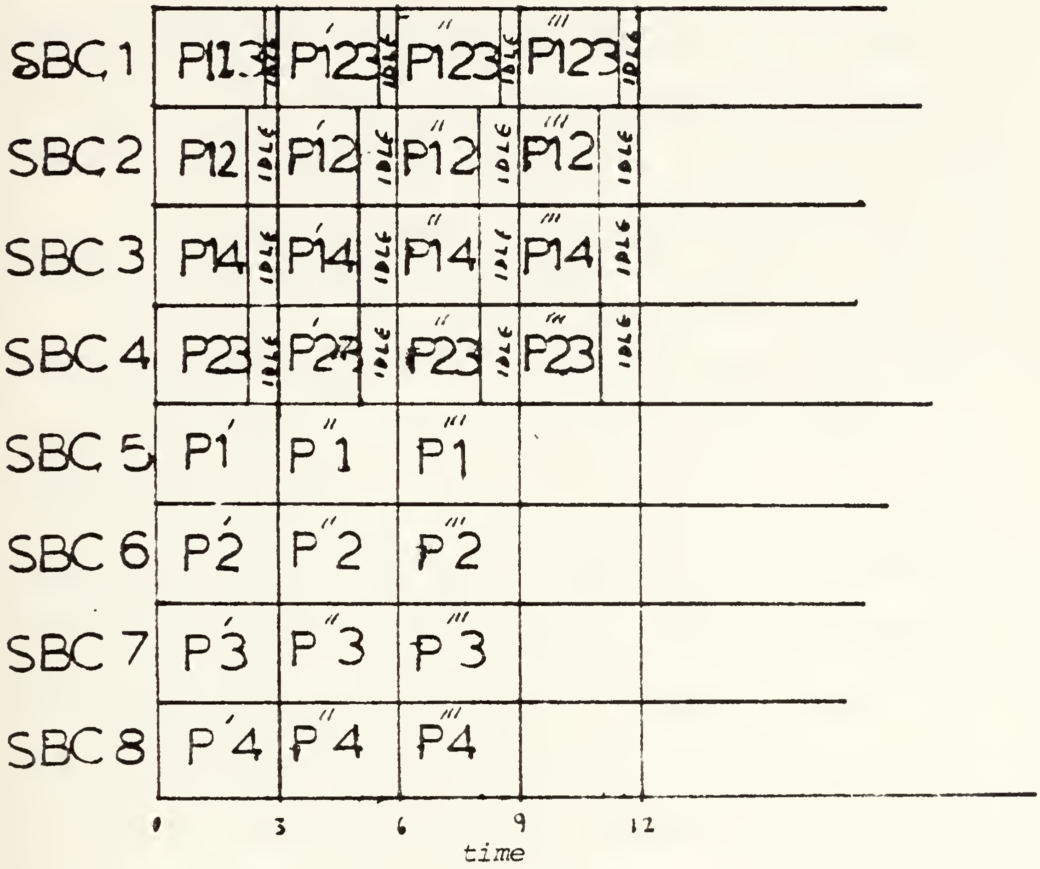


Figure V-3. Time-Line Analysis with Eight SBCs.

These response and throughput values are theoretical worst case estimates and are not confirmed by code execution. Bus use, in order to transfer data, requires some more time (in multicomputer systems). The bus access time is at the maximum approximately 5% of the execution time of each process (13 cycles out of 270 CPU cycles) as in Ref. 49 is stated.

This, for the 8 SBCs of the above example would saturate the bus at the 40% level, which would not cause substantial increase in the execution time of the processes.

The bus will become saturated when the number of SBCs executing processes in which bus access is the main instruction type is increased to 20 (100% busy). In the case of the proposed surveillance system the correlation processes altogether dedicate a total average of 10% of their execution time to bus access. So, the number of SBCs in each one of the module complexes of the multiprocessing node could be as high as 80 before a bus saturation will occur.

The same theoretical approach can be taken for the estimation of the number of module complexes that can be attached to the multiprocessing node's bus. Here, each module complex takes the place of a processor and acquires access to the bus through a private bus switch. Assuming that 5% of the traffic of the bus of the module complex is I/O to the module complex, a maximum of 20 module complexes can be attached to the multiprocessing node's bus.

The above estimates give a sense of the processing power of the multicomputer systems with multilevel bus architectures.

The difficulty faced with these systems today is that they have not been widely implemented (even if the hardware can be commercially found) and that the OS to orchestrate their operation is highly complex.

B. PERFORMANCE IMPROVEMENTS BY ADDING A NODE TO THE NETWORK

By adding more nodes to the network in order to cover the same maritime area, a different partitioning of the geographical area is required (smaller subareas). This, on one hand would simplify the calculations and reduce the response time at the node level, but would have as a result an increased number of inter-node transactions since the problem of multinode coordination will become greater. This increased number of transactions would cause greater communications delays on the ring and would reduce the responsiveness of the system as a whole.

The case where the addition of extra nodes to the network can improve the performance of the system is when an extension of the surveillance area limits is desired. Then a new subarea is added and an extra node is linked to the ring channel (an increase of the length of the ring may be required too). Such an expansion will provide the surveillance system with an expanded surveillance area and the C3 functions will be performed more extensively.

The hardware/software modifications which would be needed for the existing multiprocessing nodes are minor and isolated to the I/O modules which serve the ring interface unit. As it can be seen, the ring network is easily expandable to more nodes.

As an outline of the above discussion, the performance of the system may increase or decrease with the addition of a

new node to the ring. This depends on whether or not the new node creates substantial traffic congestion on the ring. If the ring is operating near capacity already, the addition of a node may cause a bottleneck which decreases response time on the ring. In most cases, however, the ring has excess capacity and consequently the addition of a node is easily accomplished and increases the overall performance of the system.

C. COMPARISONS WITH EXISTING SYSTEMS

Most of the currently fixed surveillance systems are based on centralized architecture concepts and suffer from the disadvantages of that system category. On the other hand, these systems are simpler in design and they do not require complicated synchronization and coordination overhead as does the distributed C3 system proposed in this thesis. A general comparison of this system with the centralized systems follows.

1. Failure Tolerance

The failure tolerance mechanisms for a centralized system are simple to design and they assume a smooth system operation. The weak point of such systems is the central (or controlling) node which, if it fails, can cause the failure of the whole system.

As has been described in the previous chapters, in the proposed system there is no controlling node with any kind of a special structure. All nodes have the same processing

power and can act as coordinating nodes or independently. This way, the failure of the ring or of an individual node will not interrupt the operation of all of the system.

At the multiprocessing node, the advantages offered by the proposed multicomputing schema are such that the system can withhold a great many hardware failures which would be hard or even impossible for a traditional computing system to cope with.

As a result of the above, the survivability of the proposed distributed surveillance system is much superior to the survivability of the centralized surveillance systems.

2. System Expansion

Centralized systems are easy to expand if there is excess capacity in I/O ports, memory and processing power. If any of these three capabilities is at its limit, a new system must be used.

The proposed system, on the other hand, is not restricted by these capacity limits. Modular expansion at the node level has theoretically no limit (by adding more levels of busing). Node expansion is easy and is done by simply adding more nodes to the ring network (at the repeater/amplifier points). However, this node expansion is somehow restricted by the capacity of the fiber-optic ring. By increasing the traffic on the ring, data transfer times become longer and the performance of the system in terms of responsiveness is degraded.

3. Programming Ease

Creating software for distributed systems, like the one proposed in this thesis, is generally more complex and time consuming than an equivalent program for a centralized computer. Fault tolerance software is complex and requires special programming skills. A larger proportion of the programmers must be familiar with writing system's programs. Systems synchronization primitives must be used throughout the code. The real-time performance requirements imposed for the proposed system add an extra level of difficulty and limit the spectrum of the programming languages that can be used.

The centralized surveillance systems are better understood because of the longer experience with them. Although the real-time synchronization problems can be more difficult in a uniprocessor case, many years of experience with time-sharing has helped to resolve these problems.

Overall, the uniprocessor centralized systems are easier to program than the proposed multicomputer system.

VI. CONCLUSIONS

A. EXTENDABILITY OF PROCESSING POWER

Throughout the description of the design of the conceptual model and its performance prediction and evaluation it has been shown that the proposed surveillance system architecture offers a granular expandability of processing power. Multicomputer architecture and surveillance task partitioning are two concepts which have contributed most to this expandability.

1. Multicomputing

The multicomputing schema of multi-level bussing that was used, has given the system an almost unlimited expansion capability. Even if the proposed system has two levels of bussing, its further expansion into lower level buses can be sustained in terms of bus capacity.

The nature of the problem has allowed this architecture to be implemented. Almost all of the computations can be performed in parallel. The limit where both the response time and throughput parameters cannot be further improved without changes in algorithms was estimated. These limits are marked by the duration of the three phases of correlation (Local data correlation, multi-sector region data correlation and cross-correlation of data coming from different generic types of sensor groups (e.g. RADAR/ESM)).

A method to predict bus saturation conditions was used, but actual calculation of the exact number of SBCs which would lead the system into such a state was not done. This requires precise timing of the execution of the software modules at the experimental level. This task constitutes a challenge for further work on the evaluation of the proposed system.

2. Area Partitioning

By partitioning the major surveillance area into four geographical subareas, the processing power of the system was increased substantially. This increase has given the proposed system the capability to process almost 4 times as much data as an equivalent centralized system during the same time span.

The ring network architecture was shown that is able to support this partitioning very efficiently and allows the addition of extra nodes to the network with a relatively low overhead.

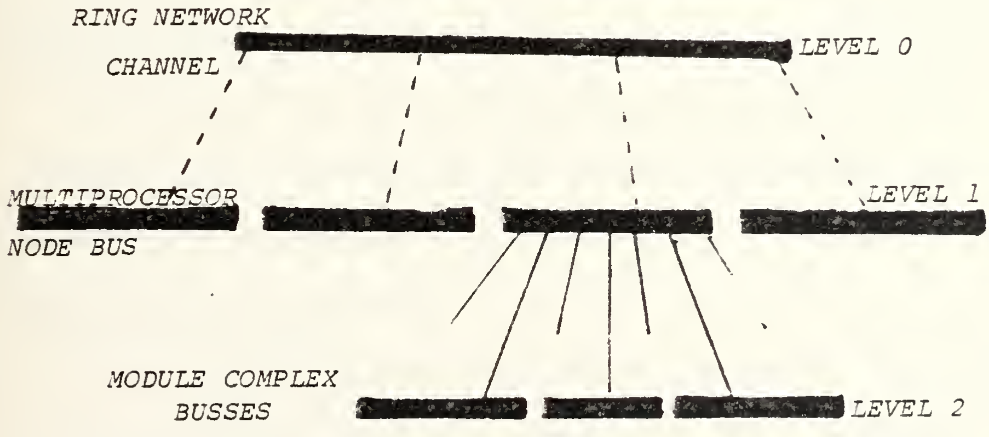


Figure VI-1. Conceptual Levels of Bussing.

Overall, the fiber-optic ring network can be viewed as a global bus which is in addition to the two levels of parallel bussing at multiprocessor and module complex level (as shown in Figure VI-1).

B. FAILURE TOLERANCE

The fault tolerance mechanisms of the proposed surveillance system have been discussed at length in the various chapters of this thesis. The main areas where special attention has been drawn are the possible major failures at the node and at the network levels.

1. Fault Tolerance at the Node Level

At the module complex level the addition of an extra number of nondedicated SBCs ensures that a hardware failure of an SBC will not create any gap in data processing and will not slow down the operation of the complex. A combined hardware/software fault tolerance mechanism permits a better handling of the high target density situations at the individual radar sectors. However, some further improvement of the method towards flexibility is believed to be possible.

The existence of a second multiprocessor node parallel bus (standby bus) allows the bus switching mechanisms of the individual module complexes to switch to it whenever the main bus experiences a failure.

Sensor failures are handled efficiently by eliminating the execution of the Multiple Common Region Correlation Modules which the failed sensor's sector covers.

Finally, by duplicating both the Local and the module complex Shared memory, the reliability of the system at the node level is substantially increased and data losses become improbable.

2. Fault Tolerance at the Network Level

A variety of failures can be sustained at the network level of the distributed system. These start from physical fiber-optic channel failures and go as far as Global Data Base (GDB) failures.

The provision for a standby ring channel for the network and the mechanisms used at the network ring interface units of the nodes, assures an uninterrupted flow of data on the network under the most probable failure conditions. The probability of fiber-optic ring saturation is minimized with the existing SLOW/FAST mechanism which reduces the traffic on the channel.

The redundancy of the GDB is an extension of the data storage backup concept adopted at the node level and ensures data availability at any instant in time. Mechanisms which are able to detect, cure, and recover from failures in the system have also been presented.

Node failures are handled as gap filling cases, where the adjacent nodes take over the control of the failed node's sensors and weapons systems.

As a result of these mechanisms and built-in backups, the fault tolerance of the system as a whole increases

substantially. Further improvements can be made in the recovery phase of each one of the failure cases.

C. MISCELLANEOUS

Node saturation, as a result of highly dense target environment in the geographic subarea it serves, is handled through the OVERLOAD/RELAXED mechanism which takes advantage of the existing alternative control lines for all the sensors and weapons systems. The control of some predefined number of the sensors is assumed by the adjacent nodes and the overloaded node is relaxed. Recovery from the saturated state needs to be elaborated in more depth.

The cost of the proposed system in comparison with the existing ones is less in terms of hardware at both the network and the node levels. In terms of software, the creation of the necessary code would require a greater and more specialized programming effort which makes the initial cost higher than for the existing systems. The advantage is that the predicted software maintenance cost is low as a result of the modularity of the design.

Physical security of information is provided through the use of underwater fiber-optic channels (main and a standby) which are very difficult to intercept without being detected.

The option that the person who is given the empire responsibility for surveillance may be stationed at any one of the subarea sites (nodes), adds a lot of operational flexibility

to the system. On the other hand, individual subarea Commander's independence is fully supported by the selected distribution schema.

The coding of the software processes of the radar module complex was partially done and no coding for the cross-correlation module complexes is included in this thesis. This makes it impossible to accurately estimate the time requirements for the completion of the whole data correlation. Only rough estimates have been given, which may substantially differ from the actual times.

D. RECOMMENDATIONS

This thesis can be characterized as a preliminary surveillance system design. Most of the principal design concepts have been discussed but many areas of the problem have not been elaborated in depth.

For the potential implementors of the proposed system, a great amount of work remains. The system is tailored to be implemented in a coastal or archipelagic ocean area where the various sensors and weapons systems can be installed on coastal, and offshore island/islet sites or on the sea bed. Power supply, maintenance, transportation, and communications requirements (other than the ring network) are also areas of concern.

For the people who would like to continue this work, a lot of coding remains to be done for both the correlation

and cross-correlation modules, and the network communications protocols. Testing of some parts of the proposed systems can be done by the use of a small number of SBCs available at most microcomputer laboratory installations.

The author of this thesis would greatly appreciate being informed of any future work on the area by mail or by being included in the distribution list of related papers and theses.

APPENDIX A: CONCEPTUAL DATA STRUCTURES AND RELATIONS

1.- Data structures

All the conceptual data types described in Chapter III, are listed below. Illustrative expression was chosen, in order to make their internal structure more understandable.

a.-

```
                           ----------
                           | TRACK |
                           ----------
                               |
     ------------------------------------------------------------
     |      |     |       |          |        |        |       |
track-no  time   size  position  heading   velocity  type   plot
            |             |
        --------    --------------
         |  |  |    |     |      |
        t1 t2 t3   pos1  pos2   pos3
                    |     |      |
                 --------------------
                 | | |  | | |   | | |
                 x y z  x y z   x y z
```

b.-

```
                           ---------
                           | TYPE |
                           ---------
                               |
                           ---------
                            |      |
                          name     id
```

```
c.-                       ---------
                          | CLASS |
                          ---------
                              |
 --------------------------------------------------------------
 |      |              |                |        |     |       |
name country op-characteristics displacement crew mission home
                       |                         |
     --------------------------------      ----------------
     |          |         |         |       |     |      |
dimensions max-speed endurance armament Off. Enlst. Civil.
     |                               |
   -----------------------      -------------------------------
   |      |       |      |      |       |       |       |    |
length breadth height draft misl#1..misl#n weapon#1..wp#m ammo
                               |                |            |
                             --------         --------     -------
                             |      |         |     |      |     |
                           name   number    name  number  amm1..ammx
```

```
d.-                      ----------
                         | SENSOR |
                         ----------
                             |
    ---------------------------------------------------------
    |           |               |               |          |
  name  passive/active  operational-char.  country  platform
                                ▼
                           -------------
                           -------------
                            .
                            .
                           -------------
```

```
e.--                     ----------
                         | WEAPON |
                         ----------
                              |
     ----------------------------------------------
     |                  |               |          |
    name      operational char.     country    platform
                       ▼                           ▼
                   ---------                   -------
                   ---------                   -------
                    .                            .
                    .                            .
                   ---------                   -------
```

f.-

```
                    ---------------
                    | NAVAL - BASE |    or   PORT
                    ---------------
                           |
 ----------------------------------------------------------------
 |        |         |          |           |          |        |
name   position  country   ships in   facilities  defense  status
          |                  port          |          |
          |                   |            |->supplies  |->AA
        -----              -------         |->provisions|->AS
        | | |              -------         |->fuel,etc. |->ASu
        x y z                 .            |->ammo      |->Land
                              .            |->repair
                           -------         |->medical
                                           |->personnel
                                           |->transportation
```

g.-

```
                    -----------
                    | AIRFIELD |      or   AIRPORT
                    -----------
                         |
 ----------------------------------------------------------------
 |        |         |          |             |          |       |
name  position  country   aircraft-in   facilities defense  status
          |                    |            |          |
        -----               -------         |->supplies   |->AA
        | | |               -------         |->provisions |->Land
        x y z                  .            |->fuel,etc.
                               .            |->ammo.
                            -------         |->repair
                                            |->medical
                                            |->personnel
                                            |->transportation
```

h.-

```
                        -------
                        | PLOT |
                        -------
                           |
   ---------------------------------------------------------
   |        |            |            |          |        |
  area  start-time   stop-time   track-list  situation scenario
                                      |                   |
                                   -------             -------
                                   -------             -------
                                      .                   .
                                      .                   .
                                   -------             -------
```

i.-

```
                                  ---------
                                  | METEO |
                                  ---------
                                      |
  -----------------------------------------------------------------------
  |       |        |        |      |      |     |       |       |      |
area start-time end-time wind temp. hum. sea precip. cloud visib.
                          |                 |                 |
                  --------        --------------        -------------
                  |       |       |      |      |       |      |      |
                 dir. strgth dir. height strgth floor ceil. eights
```

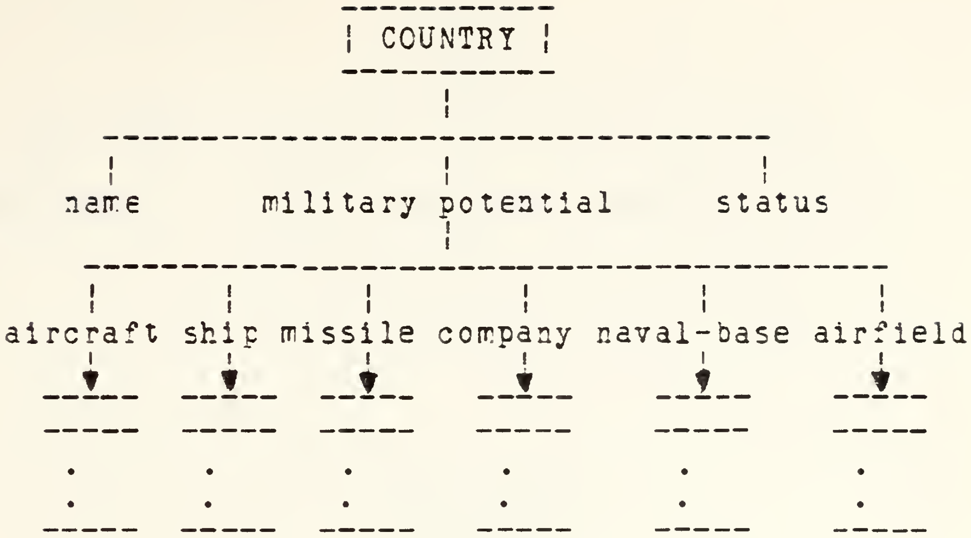
j.-

```
                              ---------------
                              | HYDROGRAPHIC |
                              ---------------
                                      |
  -------------------------------------------------------------------
  |       |        |        |    |       |        |     |      |
area start-time end-time PSR layer sea-state swell tide current
                          |                      |           |
                      ---------               -------     -------
                      |   |   |               |     |     |     |
                    LRS MRS SRS              dir. height dir. strgth
```

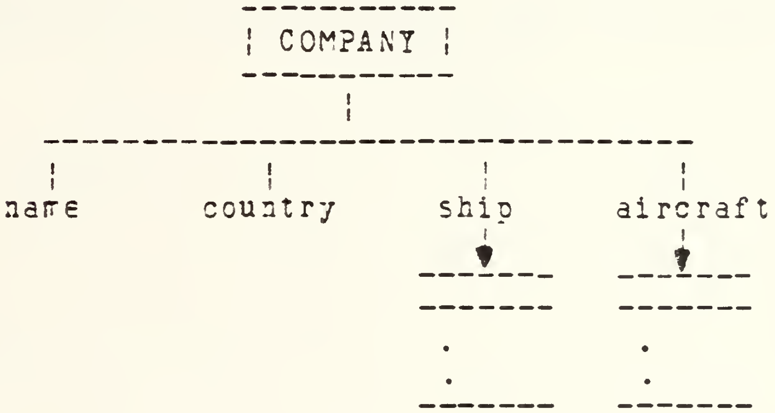
k.-

```
                            -------
                            | RCE |
                            -------
                               |
               ---------------------------------
               |          |           |        |
             number  description   time-in   next
                          |         effect     |
                          |                    |
                          v
                     ---------
                     ---------
                         .
                         .
                     ---------
```

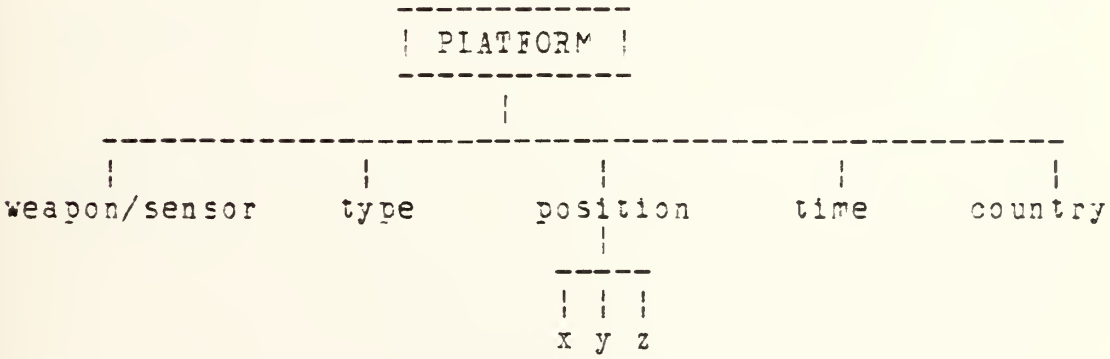
l.-


COUNTRY
name
military potential
status
aircraft
ship
missile
company
naval-base
airfield

m.-


COMPANY
name
country
ship
aircraft

n.-


PLATFORM
weapon/sensor
type
position
time
country
x
y
z

```
o.-                            --------
                               | SITE |
                               --------
                                  |
          ---------------------------------------------
          |            |          |          |          |
    weapon/sensor    type     position   country      time
                                  |
                                -----
                                | | |
                                x y z
```

```
p.-                          -----------
                             | MISSILE |
                             -----------
                                  |
        ---------------------------------------------------
        |   |      |        |         |          |        |
      name time position heading operational velocity country
                   |              character.
                   |                  |
                 -----            ---v---
                 | | |            -------
                 x y z               .
                                     .
                                  -------
```

2.- Data Relations

The conceptual relations mentioned in Chapter III, Section C are shown in the following illustrations.

a.- Type

```
                                          ---------
                                       -->| CLASS |
                                       |  ---------
                         /\            |
       --------         /  \           |
       | TYPE |---->< ISA   >----------|
       --------         \  /           |
           |             \/            |
          /\                           |  ---------
         /  \                          -->| MODEL |
        < OWNS >                          ---------
         \  /
          \/
           |
     -----------
     | COMPANY |
     -----------
```

b.- Class

```
                                          ----------
                                       -->| SENSOR |
                                       |  ----------
                         /\            |
        ---------       /  \           |
        | CLASS |-><EQUIPPED>----------|
        ---------       \  /           |
                         \/            |
                                       |  ----------
                                       -->| WEAPON |
                                          ----------
```

c.- Model

```
                                          ----------
                                       -->| SENSOR |
                                       |  ----------
                         /\            |
     ---------          /  \           |
     | MODEL |-----><EQUIPPED>---------|
     ---------          \  /           |
                         \/            |
                                       |  ----------
                                       -->| SENSOR |
                                          ----------
```

d.- Country

```
                                                  ------------
                                              -->| PLATFORM  |
                                              |   ------------
                                              |
                                              |   ------------
                                              -->| COMPANY   |
                                              |   ------------
                                              |
                                              |   ------------
                                              -->|  SITE     |
                                              |   ------------
                          /\                  |
                         /  \                 |   ---------------
 | COUNTRY |-->< HAS >-----------------------|-->| NAVAL BASE |
  -----------            \  /                 |   ---------------
   |  /\   |              \/                  |
   | /  \  |                                  |   ---------
  -<ALLIES>                                   -->| PORT  |
     \  /                                     |   ---------
      \/                                      |
                                              |   ------------
                                              -->| AIRFIELD  |
                                              |   ------------
                                              |
                                              |   ------------
                                              -->| AIRPORT   |
                                                  ------------
```

e.- Plot

```
                       /\
   --------           /  \            ---------
   | PLOT |----><CONTAINS>------| TRACK |
   --------           \  /            ---------
       |               \/
       /\
      /  \
   <CORSPND.>
      \  /
       \/
        |
   -------------
   |           |
 ---------  ----------------
 | METEO |  | HYDROGRAPHIC |
 ---------  ----------------
```

f.- Platform

```
                                    ----------
                                --->| TYPE  |
                                |   ----------
                   /\           |
                  /  \          |
-----------      /    \         |
| PLATFORM |---->< ISA >--------|
-----------      \    /         |
                  \  /          |
                   \/           |
                                |   ------------
                                --->| MISSILE |
                                    ------------
```

LIST OF REFERENCES

1. Lawson Jr., J. S., An Elementary Theory of Surveillance, Naval Electronic Systems Command, p.1, August 1978.

2. Lawson Jr., J. S., Command Control as a Process, 19th IEEE Annual Conference on Decision and Control 1980, p. 1, 1980.

3. Prokop, Jr., Computers in the Navy, Naval Institute Press, pp. 129-146, 1976.

4. Greenberg, S.A. and Williams, H.W., Reliability Aspects of Military Real-Time Command and Control Systems, MITRE Corporation's 1963 Conference Proceedings, September 1963.

5. Sittler, R. W., "An Optimal Data Association Problem in Surveillance Theory", IEEE Transactions on Military Electronics, p. 125, April 1964.

6. Naval Research Laboratory Report 8402, Naval Ocean Surveillance Correlation Handbook 1979, by I. R. Goodman and others, September 1980.

7. Naval Ocean Systems Center Technical Document 247, A Guide to U.S. Navy Command Control and Communications, by D. A. Paolucci and others, July 1979.

8. Bouchet, P., and others, "PEPIN: An Experimental Multicomputer Data Base Management System", IEEE Transactions on Computers, July 1979.

9. De Witt, D. J., "DIRECT - A Multiprocessor Organization for Supporting Relational Data Base Management Systems", IEEE Transactions on Computers, p. 395, June 1979.

10. Weitzman, C., Distributed Micro/Minicomputer Systems, Prentice Hall, 1980.

11. Barnoski, M. K. "Fiber Systems for the Military Environment", Proceedings of the IEEE, p. 1315, October 1980.

12. Reid, D. B., The Application of Multiple Target Tracking Theory to Ocean Surveillance, 18th IEEE Annual Conference on Decision and Control, p. 1046, 1979.

13. Harold, W. E. and Ohnsorge, H., "Optimal-Fiber Systems with Distributed Access", Proceedings of the IEEE, p. 1309, October 1980.

14. Burns, R. K., A Fiber-Optic Ring for Distributed Computing, Master's Thesis, Naval Postgraduate School, Monterey, California, December 1981.

15. Bradley, J., File & Data Base Techniques, CBS College Publishing, 1982.

16. Stewart, M. E., "Overview of Telecommunications Via Optical Fibers", Proceedings of the IEEE, p. 1173, October 1980.

17. Chang, K. Y., "Fiberguide Systems in the Subscriber Loop", Proceedings of the IEEE, p. 1291, October 1980.

18. Anderson, C. D. and others, "An Undersea Communications System Using Fiber-Optic Cables", Proceedings of the IEEE, p. 1299, October 1980.

19. Schwart, M. I. Gagen, P. F., and Santana, M. R., "Fiber Cable Design and Characterization", Proceedings of the IEEE, p. 1214, October 1980.

20. Nakahara, T. and Uchida, N., "Optimal Cable Design and Characterization in Japan", Proceedings of the IEEE, p. 1220, October 1980.

21. Sigel Jr., G. H., "Fiber Transmission Losses in High Radiation Fields", Proceedings of the IEEE, p. 1236, October 1980.

22. Bar-Shalom, Y., "Tracking Methods in a Multitarget Environment", IEEE Transactions on Automatic Control, p. 618, August 1978.

23. Reid, D. B., "An Algorithm for Tracking Multiple Targets", IEEE Transactions on Automatic Control, p. 843, December 1979.

24. Naval Research Laboratory Report 8340, Naval Ocean Surveillance Correlation Handbook 1978, by H. L. Wiener, and others, October 1979.

25. Morefield, C. L., Decision Directed Multitarget Techniques, 17th IEEE Conference on Decision and Control, Pacific Grove, California, p. 1195, 1978.

26. Bowman, C. L., *Maximum Likelihood Track Correlation for Multi-sensor Integration*, 18th IEEE Conference on Decision and Control, p. 374, 1979.

27. Naval Research Laboratory Memorandum Report 3949, *Correlation Algorithms in Naval Ocean Surveillance*, by H. L. Weiner, March 1979.

28. Bowman, C. L. and others, *Multisensor Multitarget Recognition and Tracking*, IEEE Asilomar Conference 1980, p. 329, 1980.

29. Bowman, C. L., *Multisensor Fusion of Target Attributes and Finematics*, IEEE Asilomar Conference 1980, p. 837, 1980.

30. Smith, M. C. and Winter, E. M., *On the Detection of Target Trajectories in a Multitarget Environment*, 17th IEEE Conference on Decision and Control, p. 1189, 1978.

31. Smith, M. C., *Feature Space Transform for Multitarget Detection*, 19th IEEE Conference on Decision and Control, p. 835, 1980.

32. Witte, F. and Lucas, D., *Probabilistic Tracking in a Multitarget Environment*, 17th IEEE Conference on Decision and Control, Pacific Grove, California, p. 1212, 1978.

33. Fortmann, T. E. and Baron, S., *Problems in Multitarget Sonar Tracking*, 17th Conference on Decision and Control, Pacific Grove, California, p. 1182, 1978.

34. Shalom-Bar, Y., Fortmann, T., and Scheffe, M., *Multitarget Tracking Using Joint Probabilistic Data Association*, 19th IEEE Conference on Decision and Control, p. 807, 1980.

35. Goodman, I. R., *A General Model for the Multiple Target Correlation and Tracking Problem*, 18th IEEE Conference on Decision and Control, p. 383, 1979.

36. Friedlander, B. and Anton, J. J., *System Identification for Multiple-Target Tracking*, IEEE Asilomar Conference, p. 360, 1980.

37. Friedlander, B., *An ARMA Modeling Approach to Multitarget Tracking*, 19th IEEE Conference on Decision and Control, p. 820, 1980.

38. Atkinson, D. A., *A Bayesian Analysis of Surveillance Attribute Data*, 19th IEEE Conference on Decision and Control, p. 826, 1980.

39. Boone, N. A., *A Multimicroprocessor Approach to Simulate I/O for the Aegis AN/SPY-1A Radar Controller*, Master's Thesis, pp. 95-296, Naval Postgraduate School, Monterey, California, 1981.

40. Jones, A. K. and Scharz, "Experience Using Multiprocessor Systems, A Status Report", *ACM Computer Surveys*, June 1980.

41. Kodres, U. R., *Processing Efficiency of a Class of Multicomputer Systems*, Proceedings of the ISMM International Symposium, Cambridge, Massachusetts, July 1982.

42. Sandel, N. R., Lauer, G., and Kramer, L., *Research Issues in Surveillance for C3*, 19th IEEE Conference on Decision and Control, p. 201, 1980.

43. Minoura, T. and Wiedrhold, G., "Resilient Extended True-Copy Token Scheme for a Distributed Data Base System", *IEEE Transactions on Software Engineering*, p. 173, May 1982.

44. Wittie, L. D., "Communications Structures for Large Networks Microcomputers", *IEEE Transactions on Computers*, p. 264, April 1981.

45. Jafari, H., Lewis, T. G. and Spragins, J. D., "Simulation of a Class of Ring-Structured Networks", *IEEE Transactions on Computers*, p. 385, May 1980.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Library, Code 0142 Naval Postgraduate School Monterey, CA 93940	2
2.	Department Chairman, Code 52Hq Department of Computer Science Naval Postgraduate School Naval Postgraduate School Monterey, CA 93940	1
3.	Hellenic Navy Command Communications Section Cholargos, Stratopedon Papagou Athens, Greece	2
4.	Professor Uno R. Kodres, Code 52Kr Department of Computer Science Naval Postgraduate School Monterey, CA 93940	1
5.	Professor D. Badal, Code 52Zd Department of Computer Science Naval Postgraduate School Monterey, CA 93940	1
6.	Professor Yiannis Vassiliou New York University Graduate School of Business Administration 100 Trinity Place New York, NY 10006	1
8.	Commander Stavros Vassiliou, HN Hellenic Naval Tactical School Stratopedon Kanellopoulos Scaramangas, Pireus, Greece	2
9.	Commander Panagiotis Loumakis, HN Hellenic Navy Command Cholargos, Stratopedon Papagou Athens, Greece	1

10.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22314	2

Thesis 199656
V3423 Vassiliou
c.1 A distributed network supporting ocean surveillance.

26 NOV 83 27906
19 SEP 84 13423

Thesis 199656
V3423 Vassiliou
c.1 A distributed network supporting ocean surveillance.

thesV3423
A distributed network supporting ocean s
3 2768 002 05407 4
DUDLEY KNOX LIBRARY